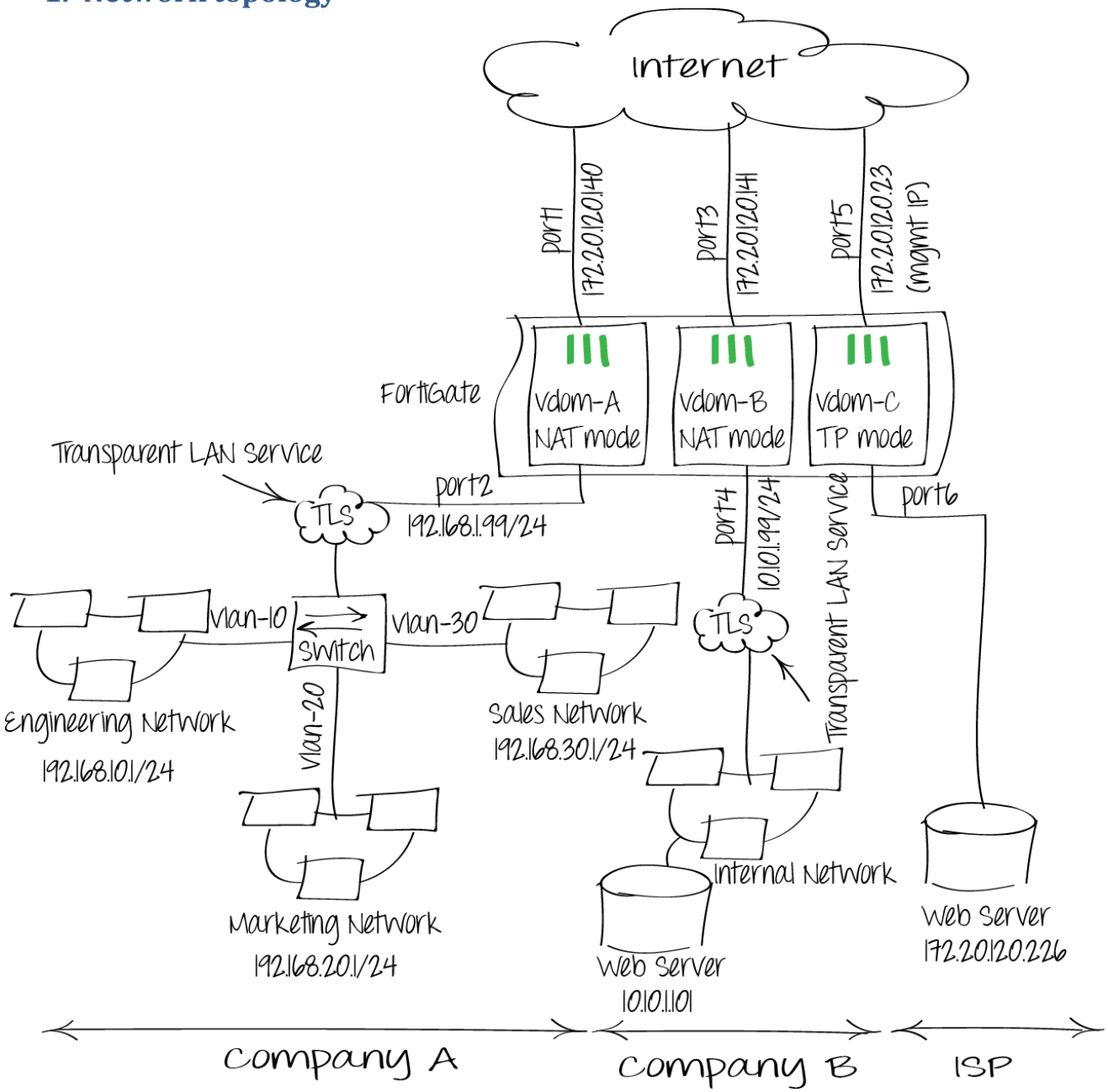
Hosting more than one FortiOS instance on a single FortiGate unit using VDOMs and VLANs

1. Network topology



Use Virtual domains (VDOMs) to divide the FortiGate unit into two or more virtual instances of FortiOS that function similar to independent FortiGate units. Each VDOM has its own physical interfaces, routing configuration, and security policies.

This example simulates an ISP that provides Company A and Company B with Internet services and offer to them daily network management and security via TLS (Transparent LAN Service) connections. Also the ISP needs to protect its servers set to public routeable IP addresses.
Each company would have its own Internet IP address and internal network. This configuration requires:

- Two VDOMs: VDOM-A and VDOM-B operating in NAT/Route mode, VDOM-A for company A and VDOM-B for company B
- One VDOM-C operating in transparent mode for the ISP

This scenario will cover the following features:

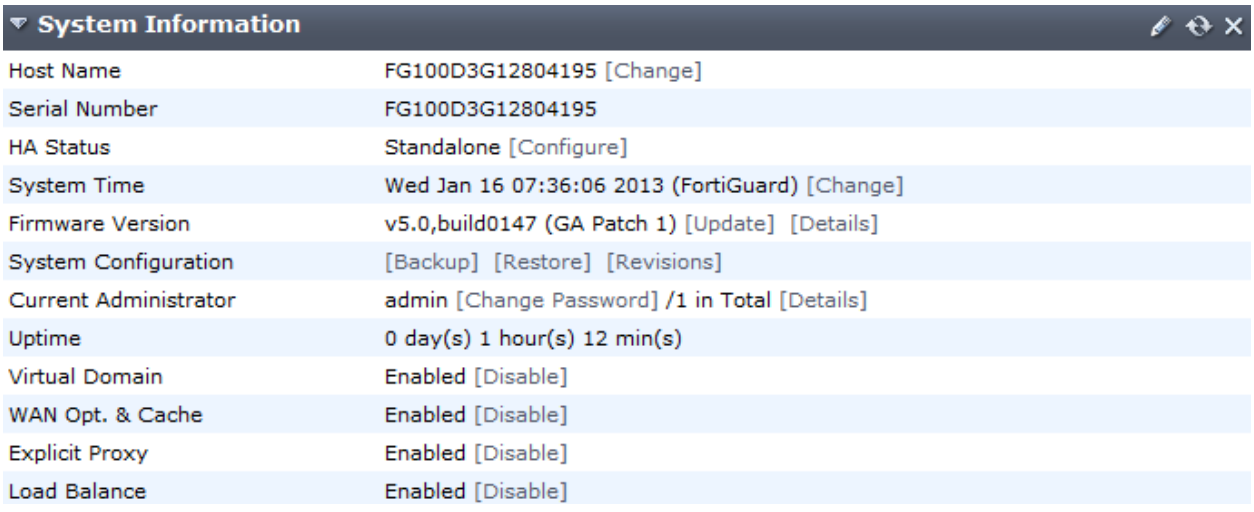
- VDOM-A:
  - Setting up VLANS to separate internal networks
  - Configure DHCP server on VLAN interface

- VDOM-B:
  - Configure local DNS server resolving internal web sites and servers
  - Use DHCP to assign some IPs according to device MAC addresses
  - Configure traffic shaping for sensitive traffic
  - Configure explicit web proxy and web caching on some network

- VDOM-C:
  - Allowing secure access to a web servers set to public IP address
  - Protecting this web server using UTM security profiles

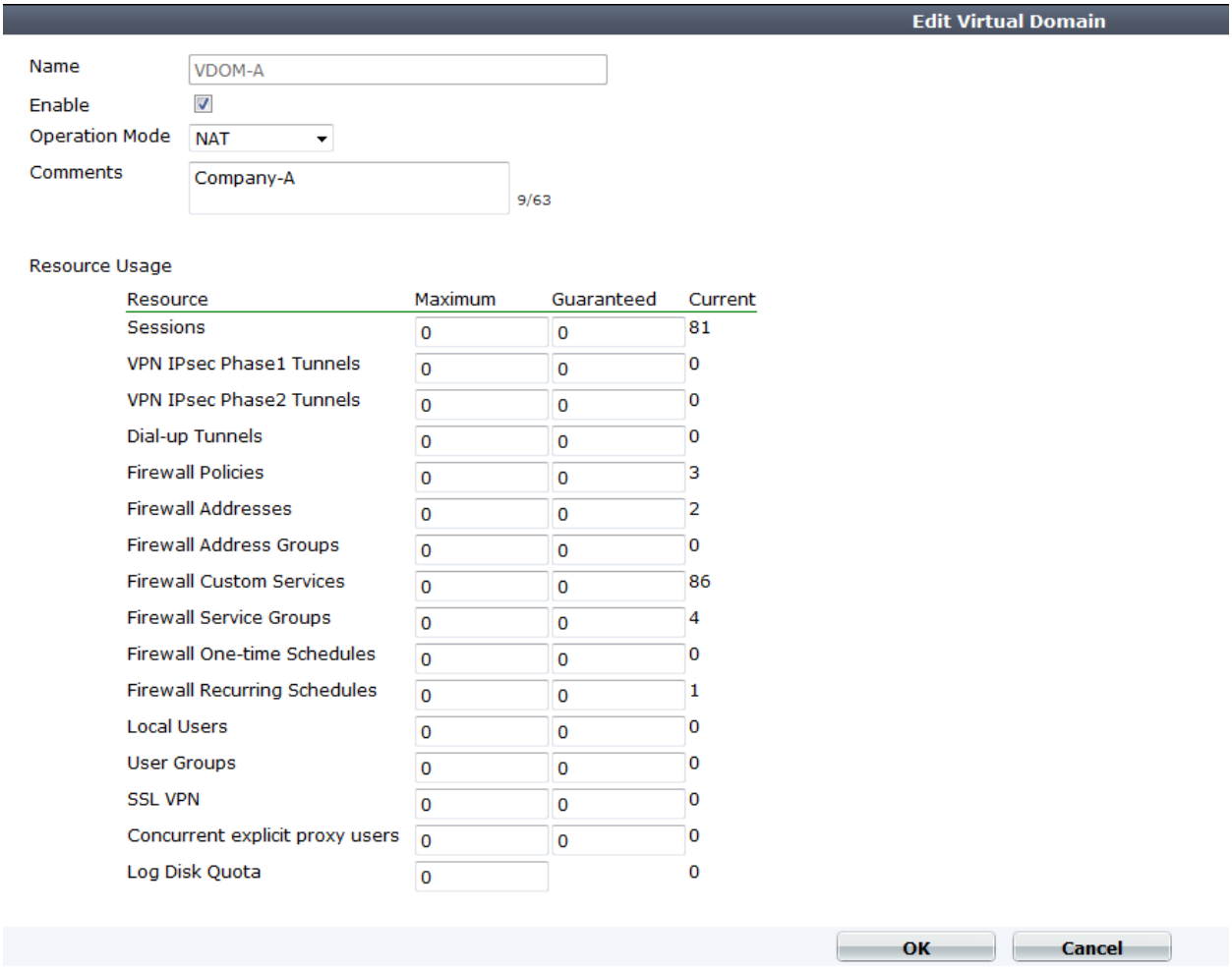
2. Creating VDOM-A, VDOM-B and VDOM-C

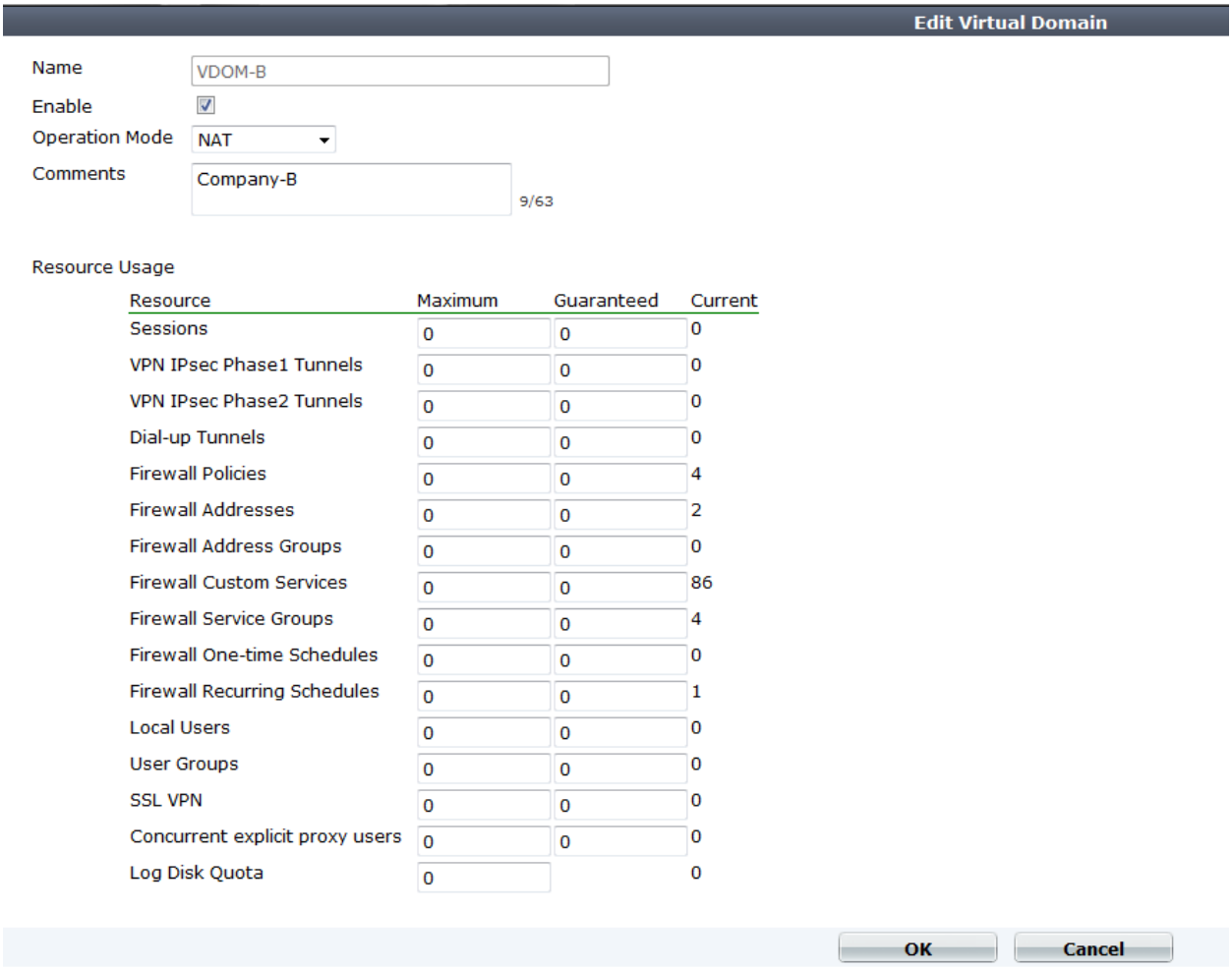
Go to System > Dashboard > Status and enable Virtual Domain

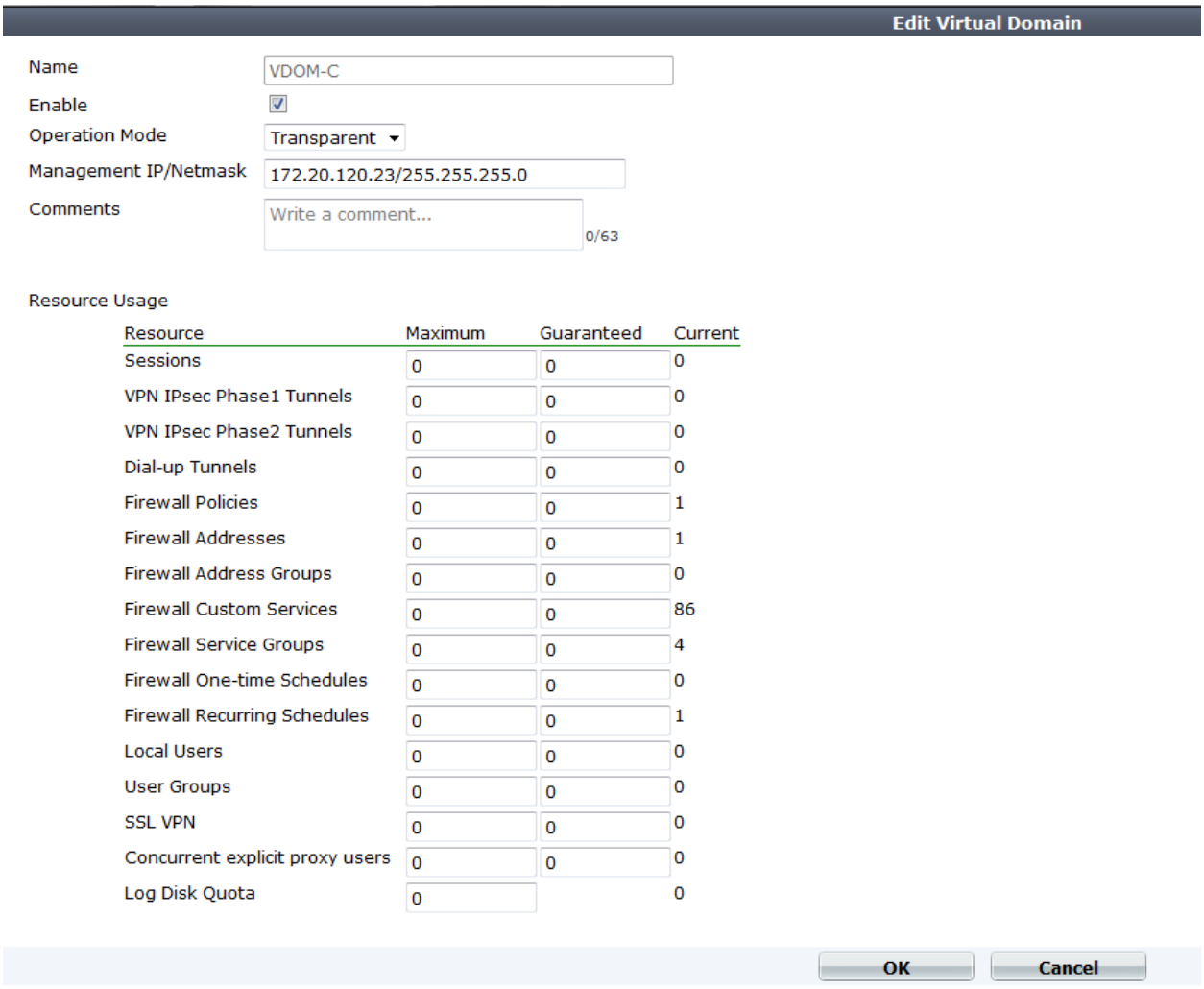


System Information	
Host Name	FG100D3G12804195 [Change]
Serial Number	FG100D3G12804195
HA Status	Standalone [Configure]
System Time	Wed Jan 16 07:36:06 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0147 (GA Patch 1) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	0 day(s) 1 hour(s) 12 min(s)
Virtual Domain	Enabled [Disable]
WAN Opt. & Cache	Enabled [Disable]
Explicit Proxy	Enabled [Disable]
Load Balance	Enabled [Disable]

Go to Global > VDOM > VDOM and add VDOM-A, VDOM-B, VDOM-C and a management IP for VDOM-C since it's transparent



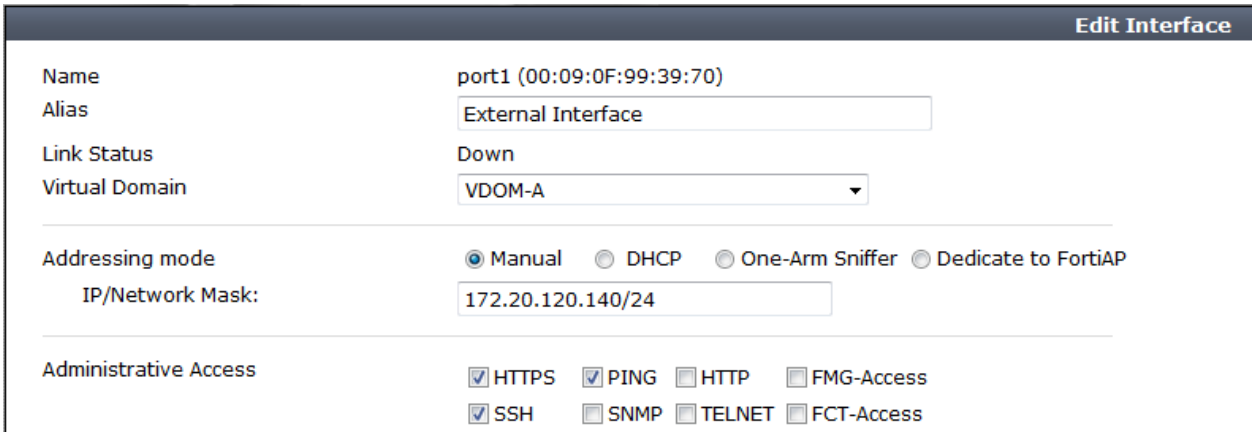

Edit Virtual Domain
Name
VDOM-B
Enable
Operation Mode
NAT
Comments
Company-B
9/63
Resource Usage
Resource
Maximum
Guaranteed
Current
Sessions
0
0
0
VPN IPsec Phase1 Tunnels
0
0
0
VPN IPsec Phase2 Tunnels
0
0
0
Dial-up Tunnels
0
0
0
Firewall Policies
0
0
4
Firewall Addresses
0
0
2
Firewall Address Groups
0
0
0
Firewall Custom Services
0
0
86
Firewall Service Groups
0
0
4
Firewall One-time Schedules
0
0
0
Firewall Recurring Schedules
0
0
1
Local Users
0
0
0
User Groups
0
0
0
SSL VPN
0
0
0
Concurrent explicit proxy users
0
0
0
Log Disk Quota
0
0
OK
Cancel

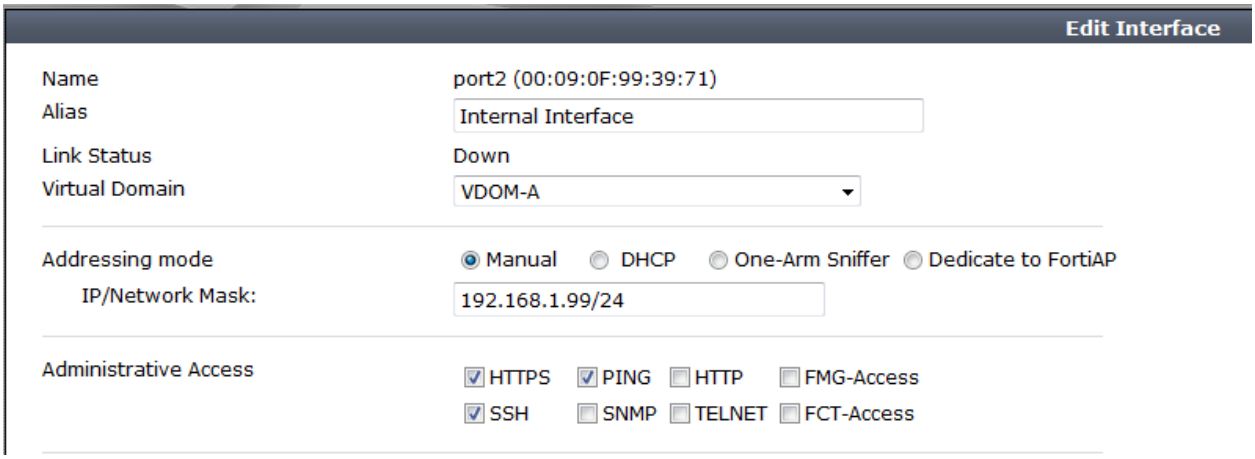


By default, root is the management VDOM and it should have an interface connected to the internet for management traffic such as FortiGuard services, NTP, SNMP, etc. the management VDOM can be moved to VDOM-A or VDOM-B or VDOM-C.

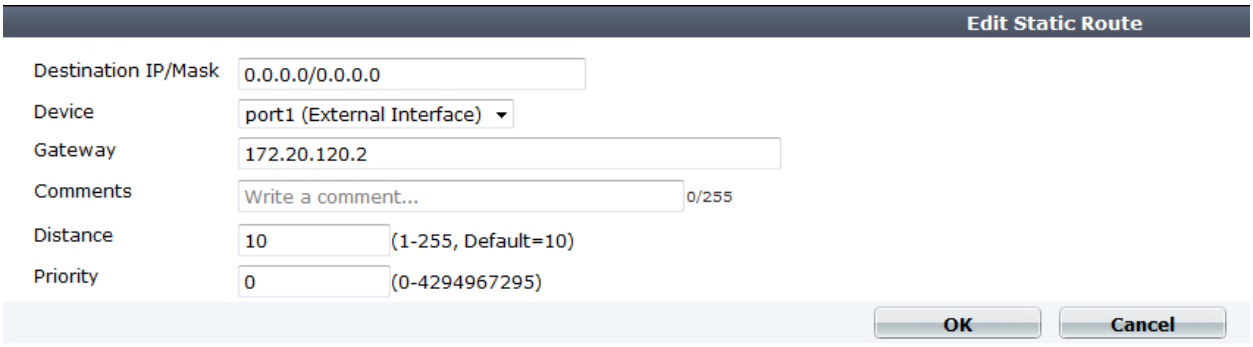
The admin account has full control of all VDOMs in the FortiGate unit. Admin account can access the FortiGate on any interface of any VDOM as far as the interface has an IP address and allowing https access.

Go to Global > Network > Interface and add port1 and port2 to VDOM-A

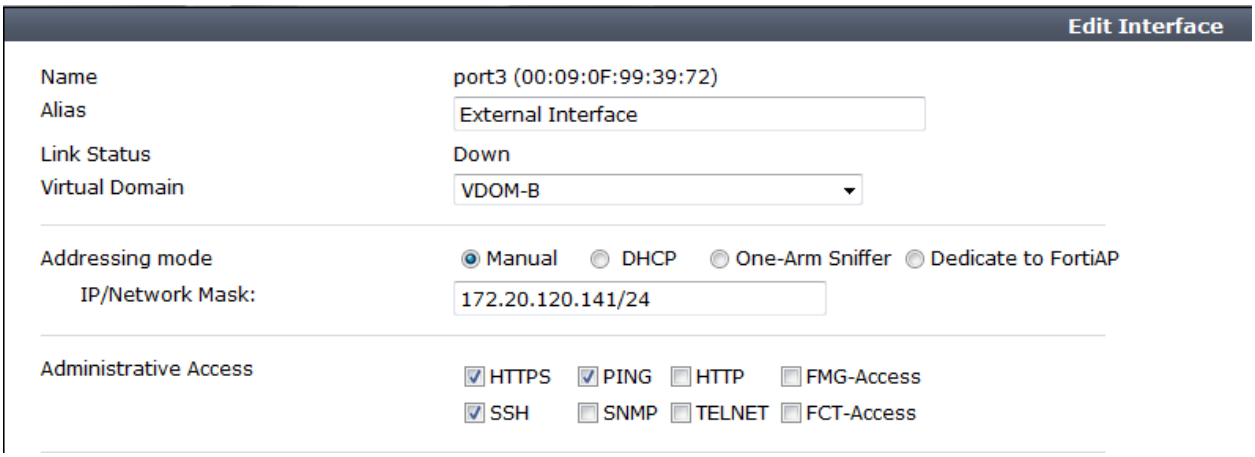


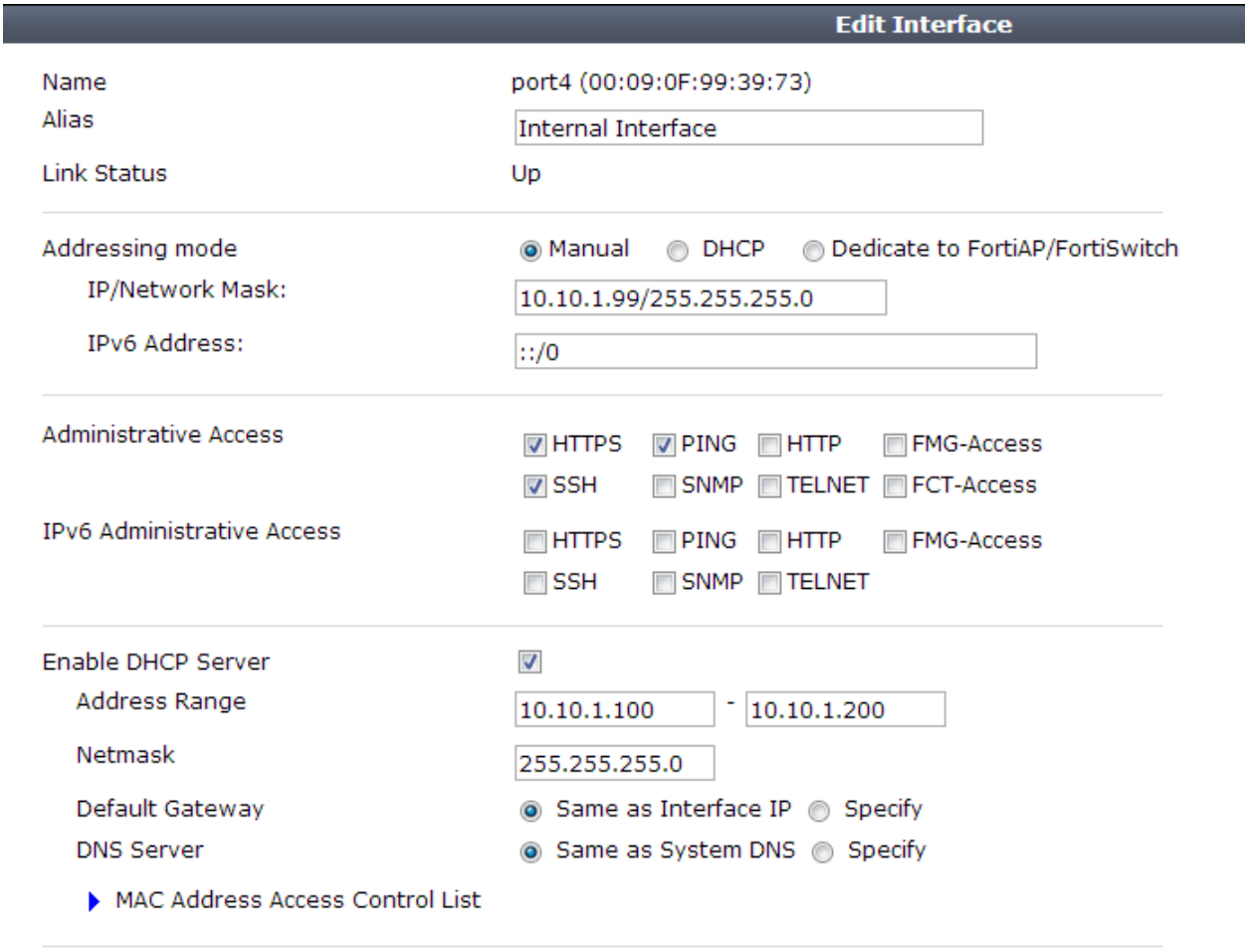


Go to Router > Static > Static Route to add a default route for VDOM-A

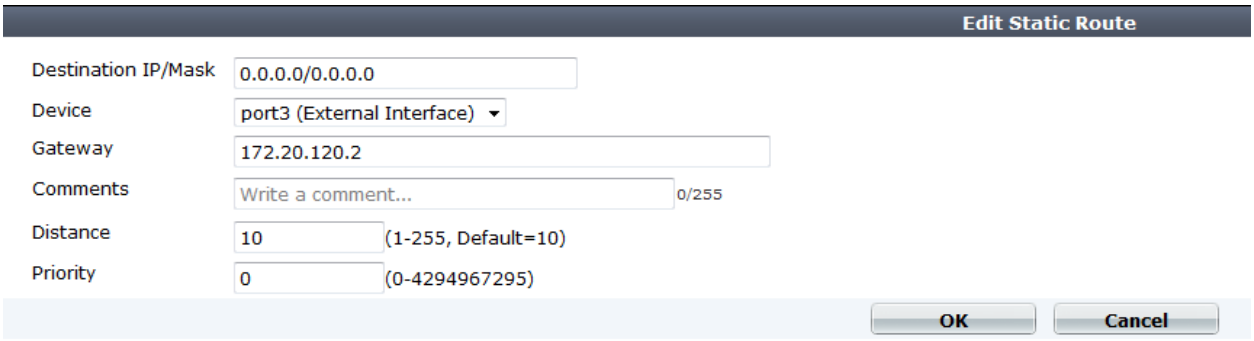


Go to Global > Network > Interface and add port3 and port4 to VDOM-B, and add DHCP server to port4

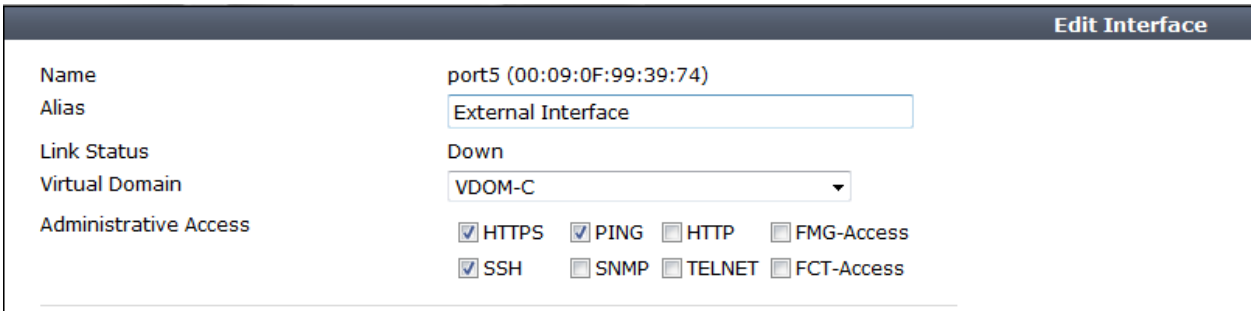


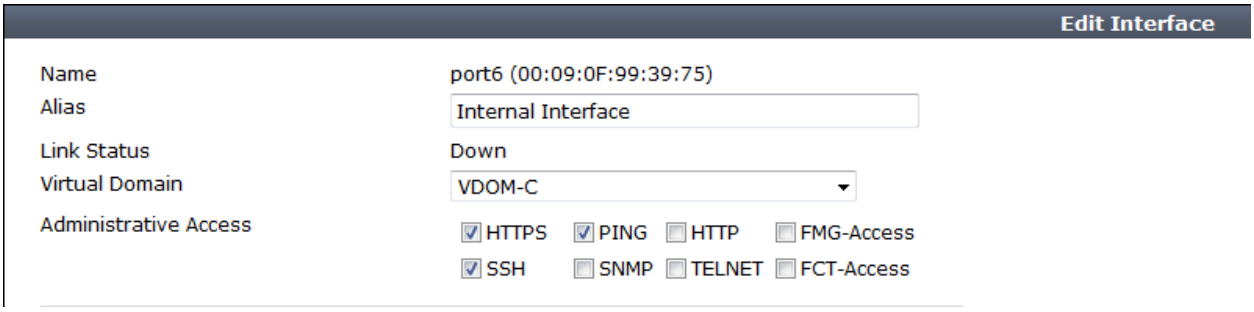


Go to Router > Static > Static Route to add a default route for VDOM-B



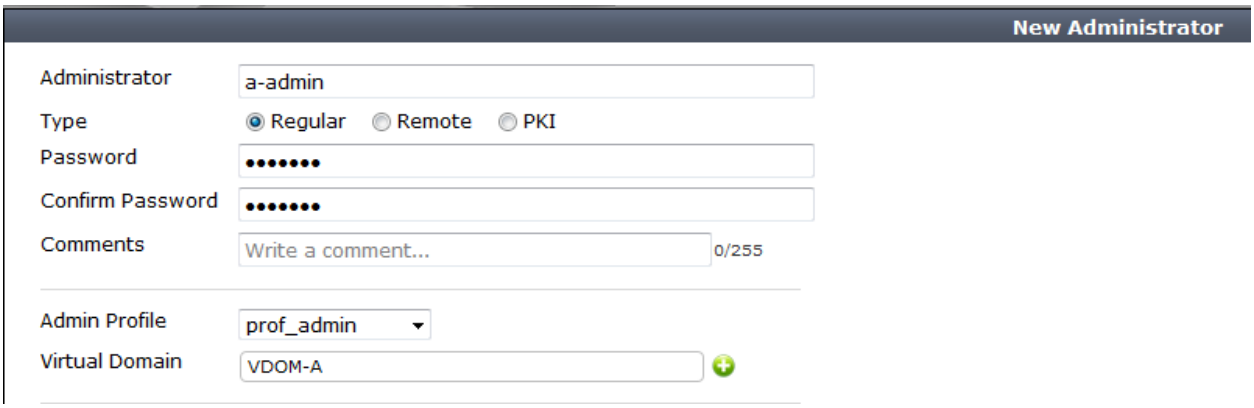
Go to Global > Network > Interface and add port5 and port6 to VDOM-C

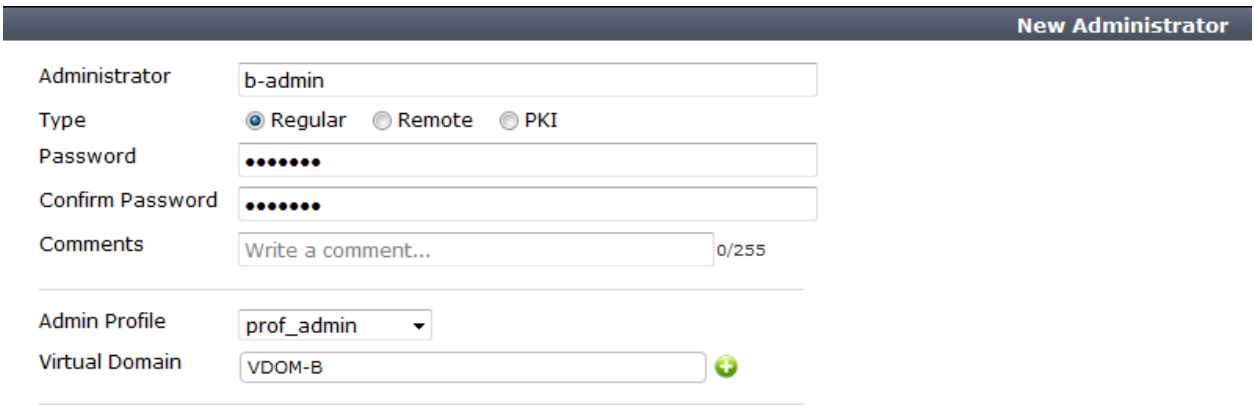


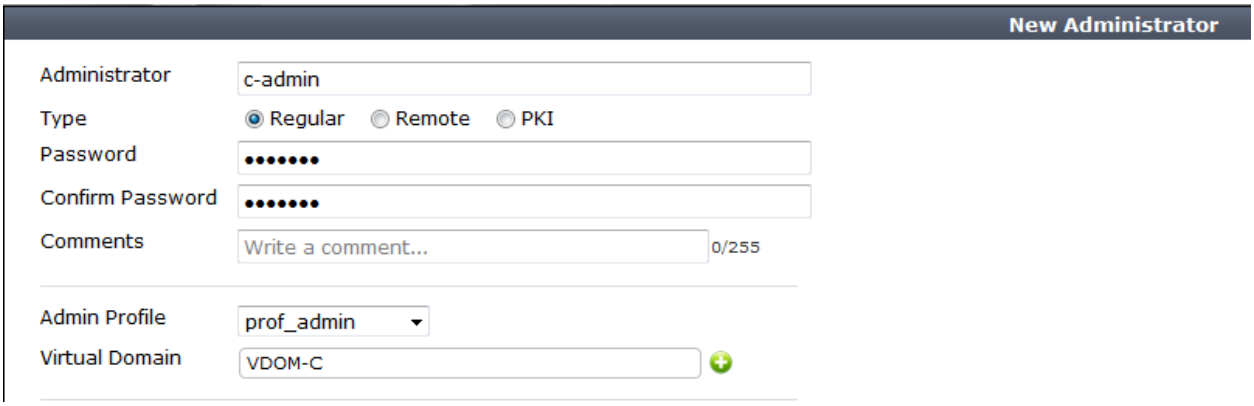


Go to System > Network > Routing Table to add a default route for VDOM-C

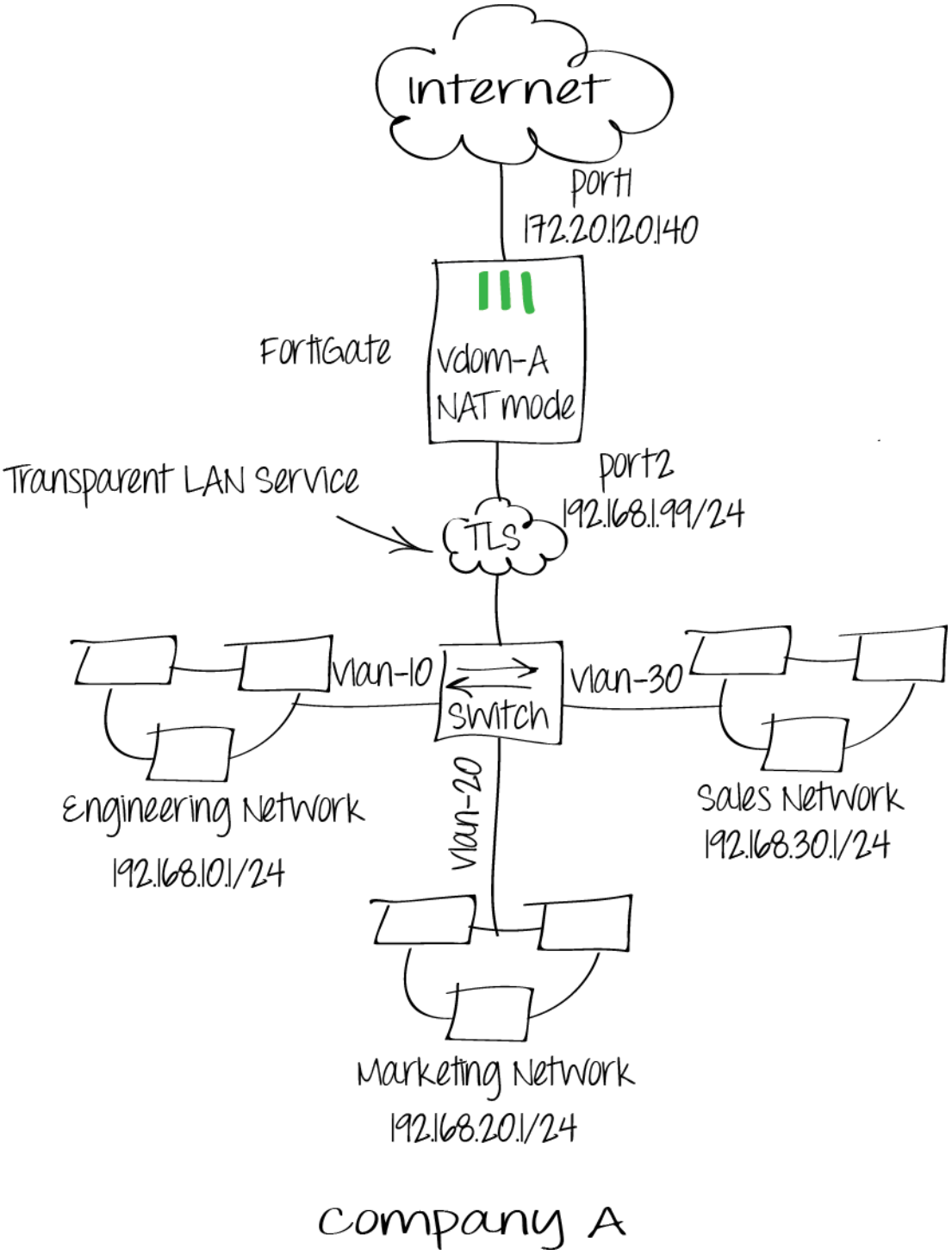
Go to Global > Admin > Administrators to create administrators for each VDOM. The administrators should only have access to their own


New Administrator
Administrator
a-admin
Type
Regular
Remote
PKI
Password
Confirm Password
Comments
Write a comment...
0/255
Admin Profile
prof_admin
Virtual Domain
VDOM-A


New Administrator
Administrator
b-admin
Type
Regular
Remote
PKI
Password
Confirm Password
Comments
Write a comment...
0/255
Admin Profile
prof_admin
Virtual Domain
VDOM-B


New Administrator
Administrator
c-admin
Type
Regular
Remote
PKI
Password
Confirm Password
Comments
Write a comment...
0/255
Admin Profile
prof_admin
Virtual Domain
VDOM-C

3. Configuring VDOM-A using VLANs



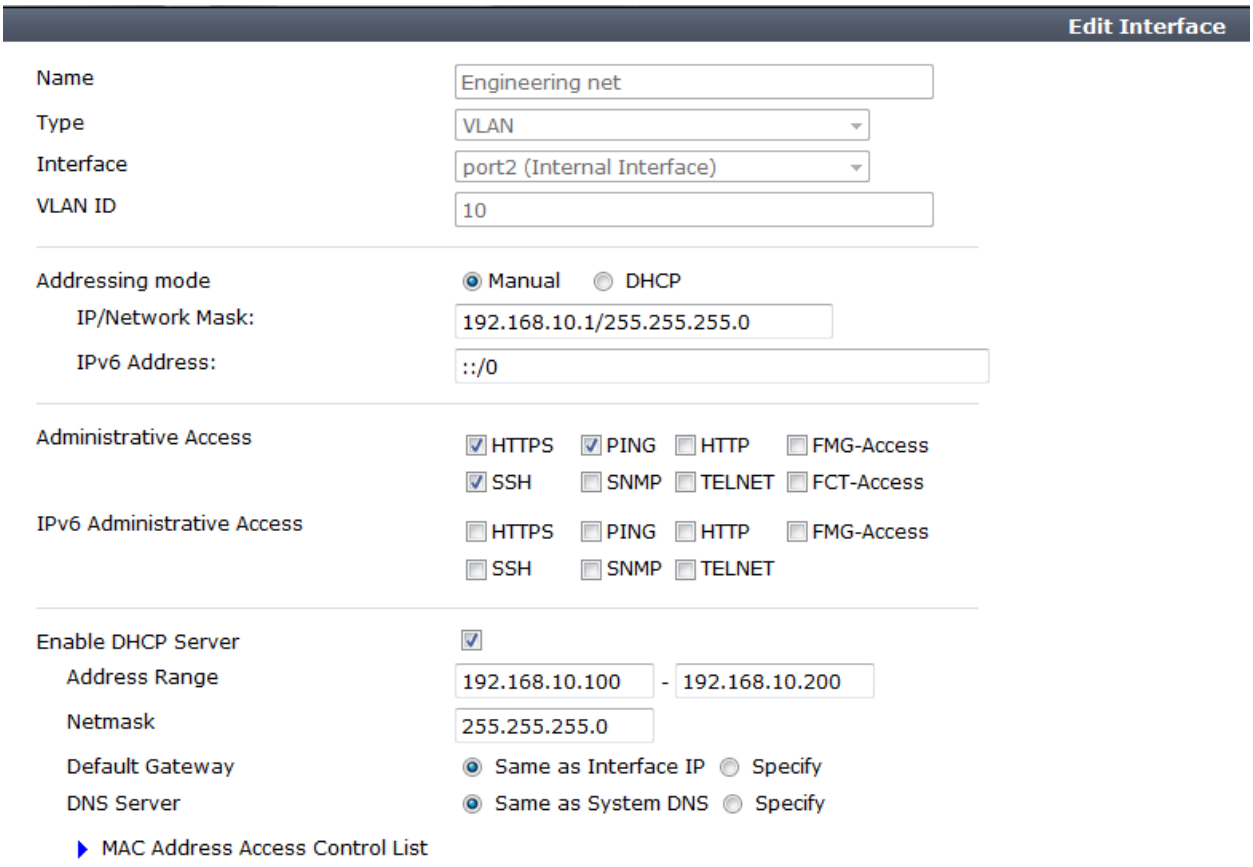
Log on to the FortiGate unit VDOM-A on port1 or port2 interface using a-admin account, this will let you manage only VDOM-A

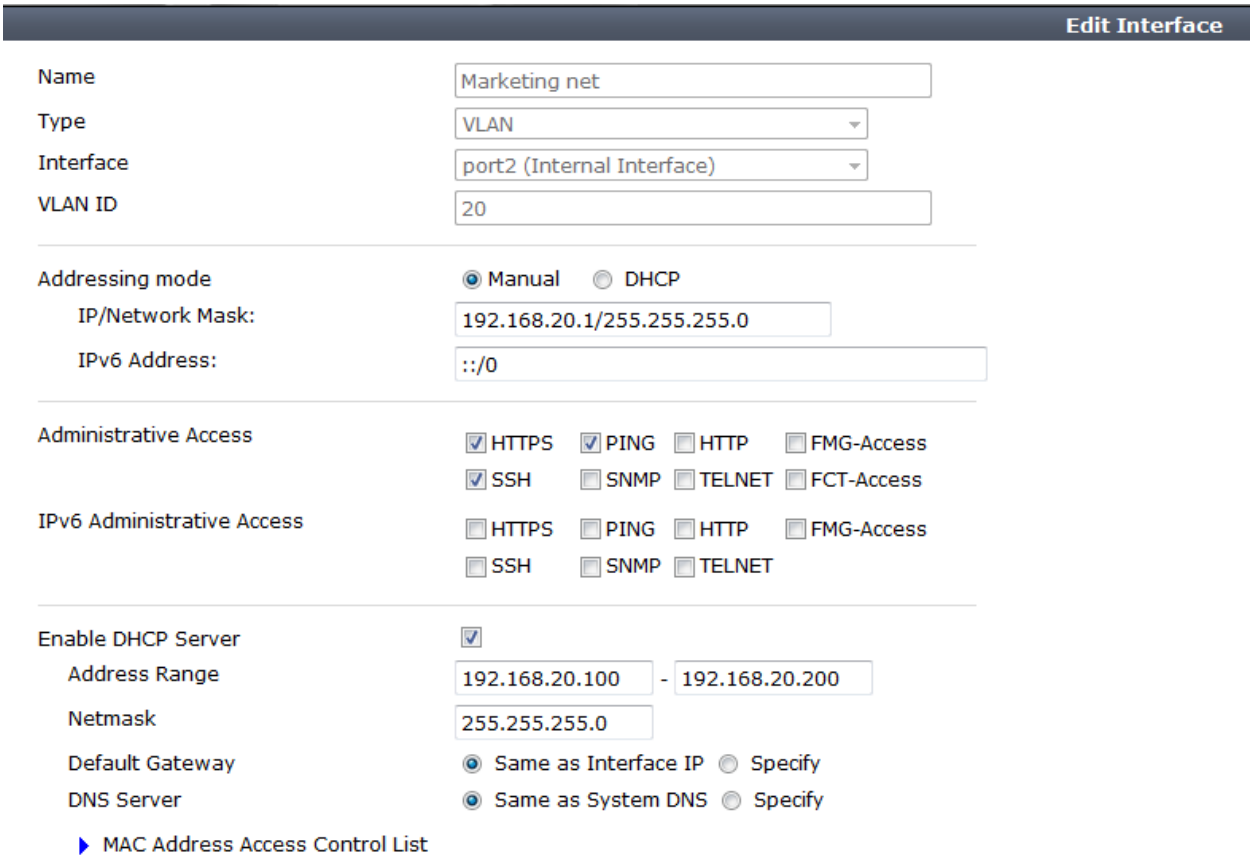
Company A separates their three internal networks (engineering, sales and marketing) using VLANs
This solution uses VLANs to connect three networks to VDOM-A internal interface in the following way:

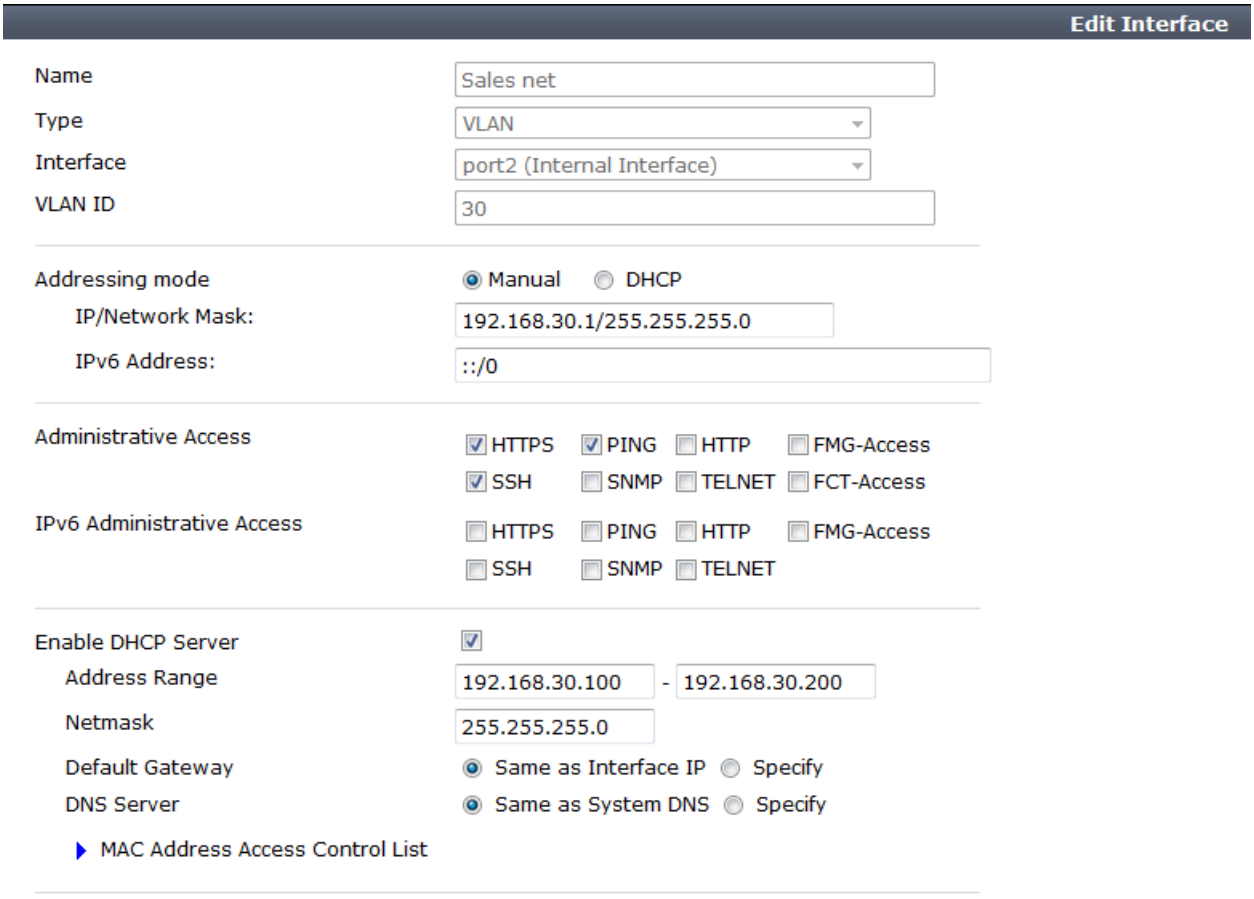
- Packets from each network pass through a VLAN switch before reaching the VDOM-A . The VLAN switch adds different VLAN tags to packets from each network.
- To handle VLANs on VDOM-A, add VLAN interfaces to the internal interface for each network
- Add a DHCP server to each VLAN interface.
- Create security policies to allow each network to access the Internet.

This solution assumes you have configured a VLAN switch to tag packets from the three networks

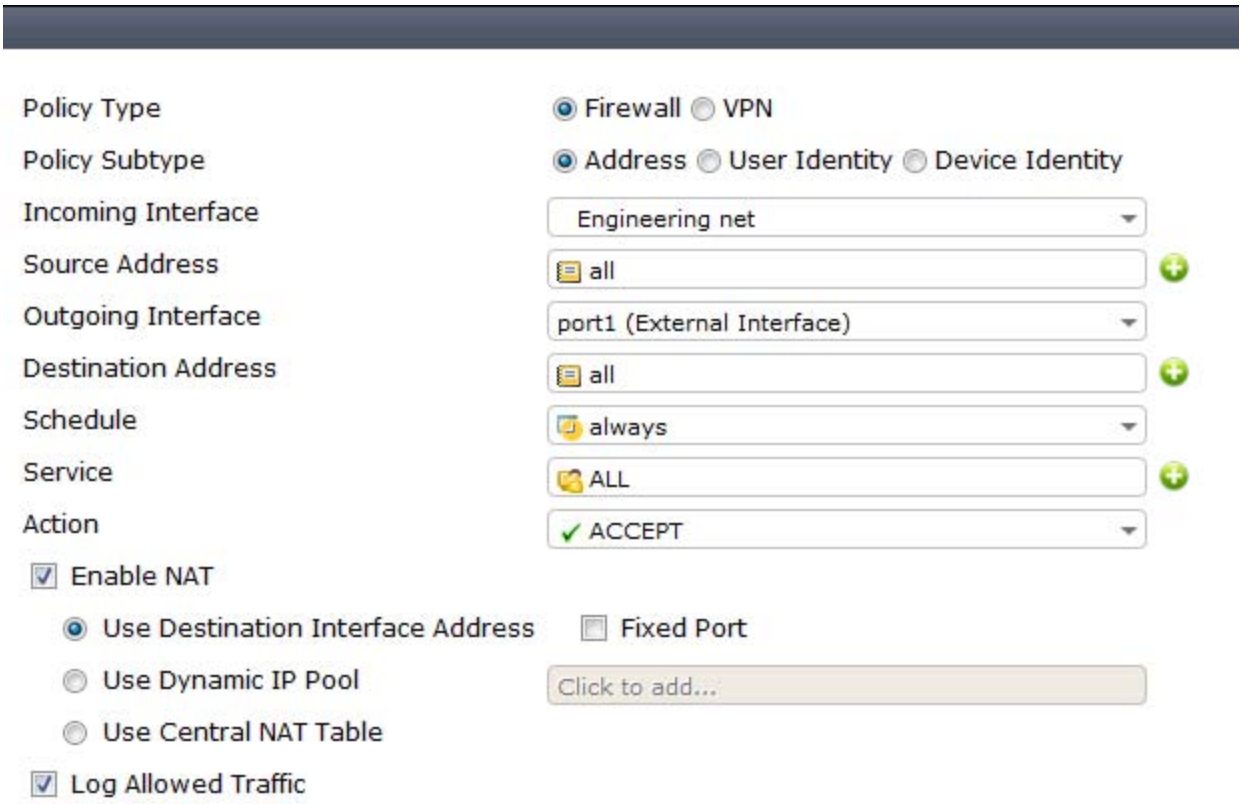
Go to System > Network > Interface to create three new vlan interfaces for engineering, marketing and sales networks

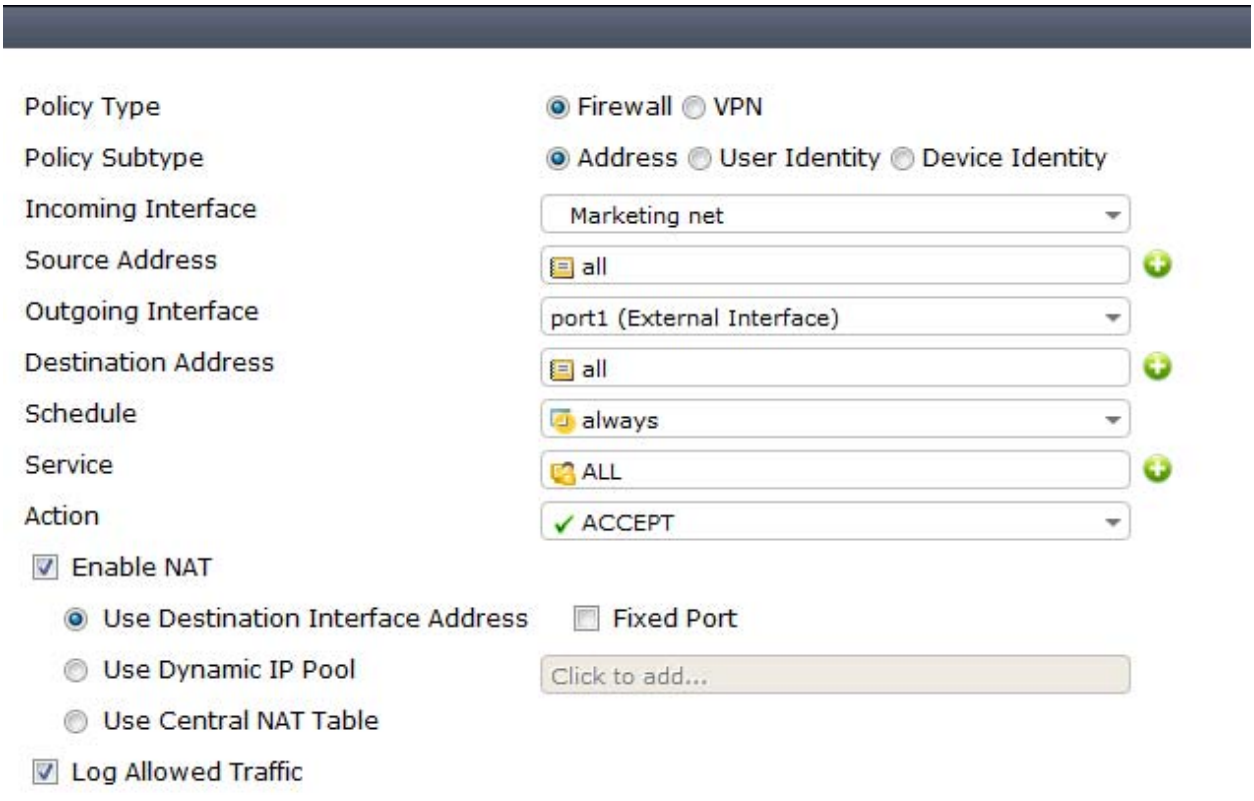


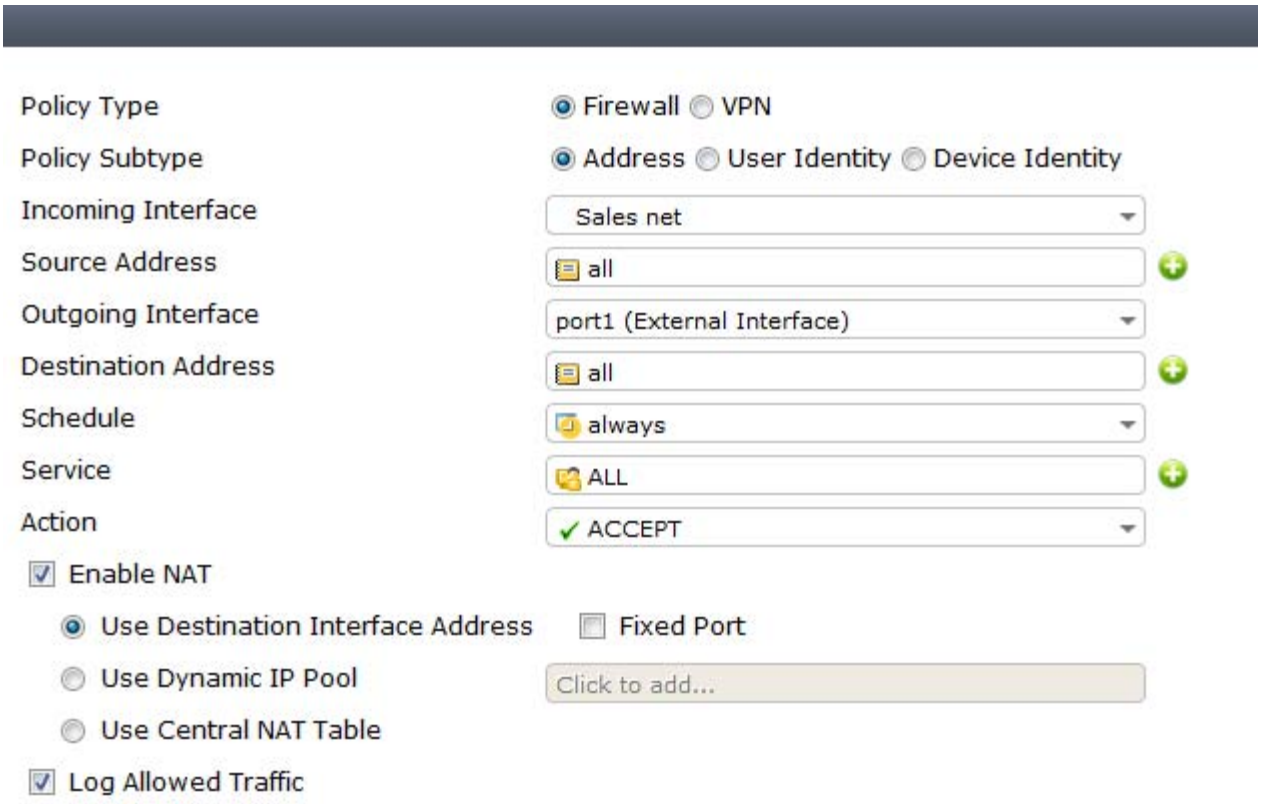

Edit Interface
Name
Marketing net
Type
VLAN
Interface
port2 (Internal Interface)
VLAN ID
20
Addressing mode
Manual
DHCP
IP/Network Mask:
192.168.20.1/255.255.255.0
IPv6 Address:
::/0
Administrative Access
HTTPS
PING
HTTP
FMG-Access
SSH
SNMP
TELNET
FCT-Access
IPv6 Administrative Access
HTTPS
PING
HTTP
FMG-Access
SSH
SNMP
TELNET
Enable DHCP Server
Address Range
192.168.20.100
-
192.168.20.200
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Specify
MAC Address Access Control List



Go to Policy > Policy > Policy to add firewall policies that allows users on the engineering, marketing and sales networks to access the internet separately


Policy Type
Firewall
VPN
Policy Subtype
Address
User Identity
Device Identity
Incoming Interface
Engineering net
Source Address
all
Outgoing Interface
port1 (External Interface)
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Enable NAT
Use Destination Interface Address
Fixed Port
Use Dynamic IP Pool
Click to add...
Use Central NAT Table
Log Allowed Traffic


Policy Type
Firewall
VPN
Policy Subtype
Address
User Identity
Device Identity
Incoming Interface
Marketing net
Source Address
all
Outgoing Interface
port1 (External Interface)
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Enable NAT
Use Destination Interface Address
Fixed Port
Use Dynamic IP Pool
Click to add...
Use Central NAT Table
Log Allowed Traffic



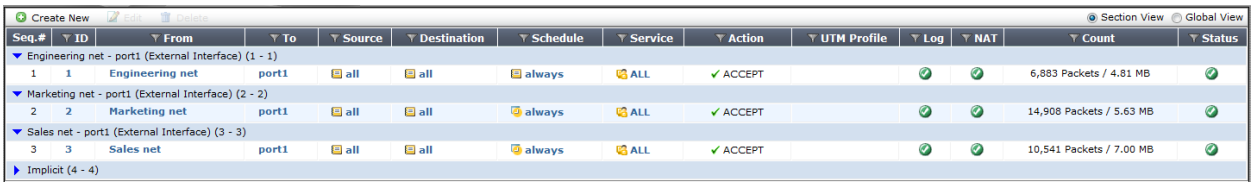
4. Showing results

From engineering network set all hosts IPs in the same subnet as the “Engineering net” vlan (192.168.10.x/24) with the gateway 192.168.10.1 or set hosts to use DHCP

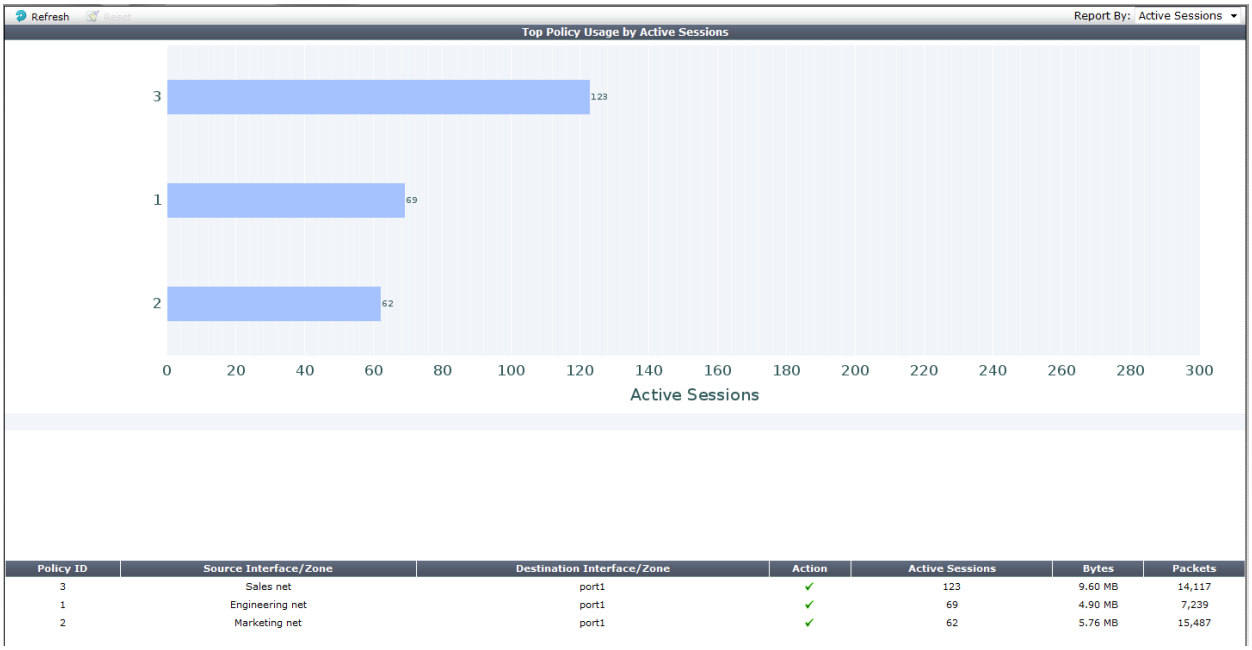
From marketing network set all hosts IPs in the same subnet as the “Marketing net” vlan (192.168.20.x/24) with the gateway 192.168.20.1 or set hosts to use DHCP
And from sales network set all hosts IPs in the same subnet as the “Sales net” vlan (192.168.30.x/24) with the gateway 192.168.30.1 or set hosts to use DHCP

Then users from any of the networks should be able to connect to the Internet

Policy > Policy > Policy to see traffic count for each firewall policy

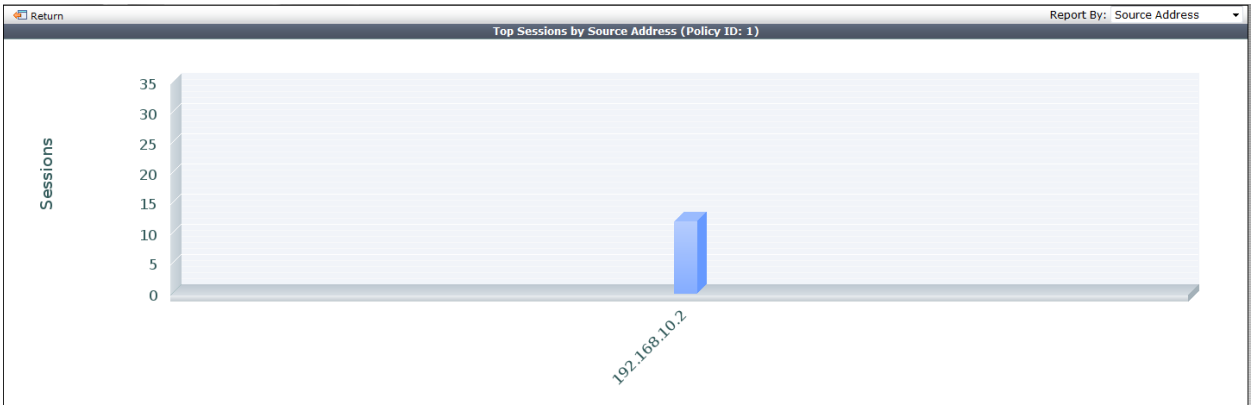


Go to Policy > Monitor > Policy Monitor to see the active sessions

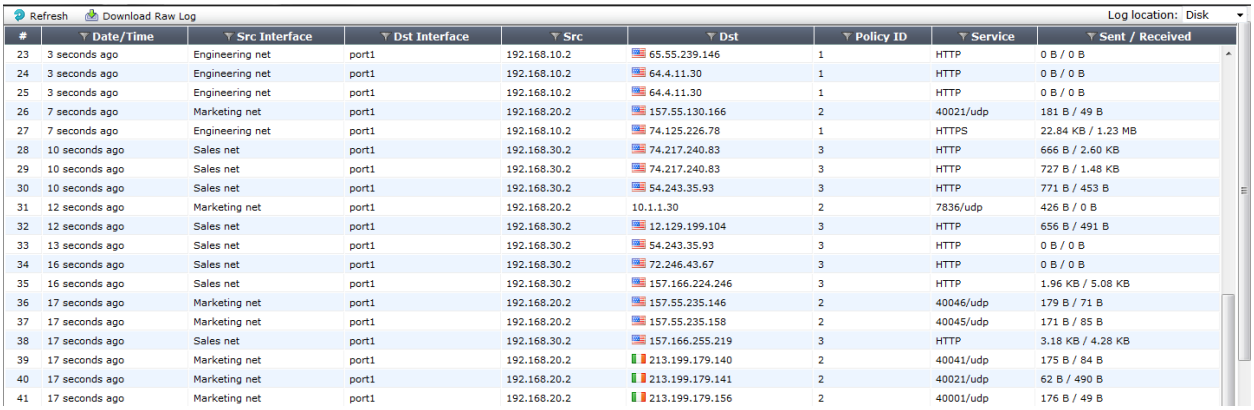


Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
3	Sales net	port1	✓	123	9.60 MB	14,117
1	Engineering net	port1	✓	69	4.90 MB	7,239
2	Marketing net	port1	✓	62	5.76 MB	15,487

Click on each blue bar for details for source IP and policy Id



Go to Log & Report > Traffic Log > Forward Traffic

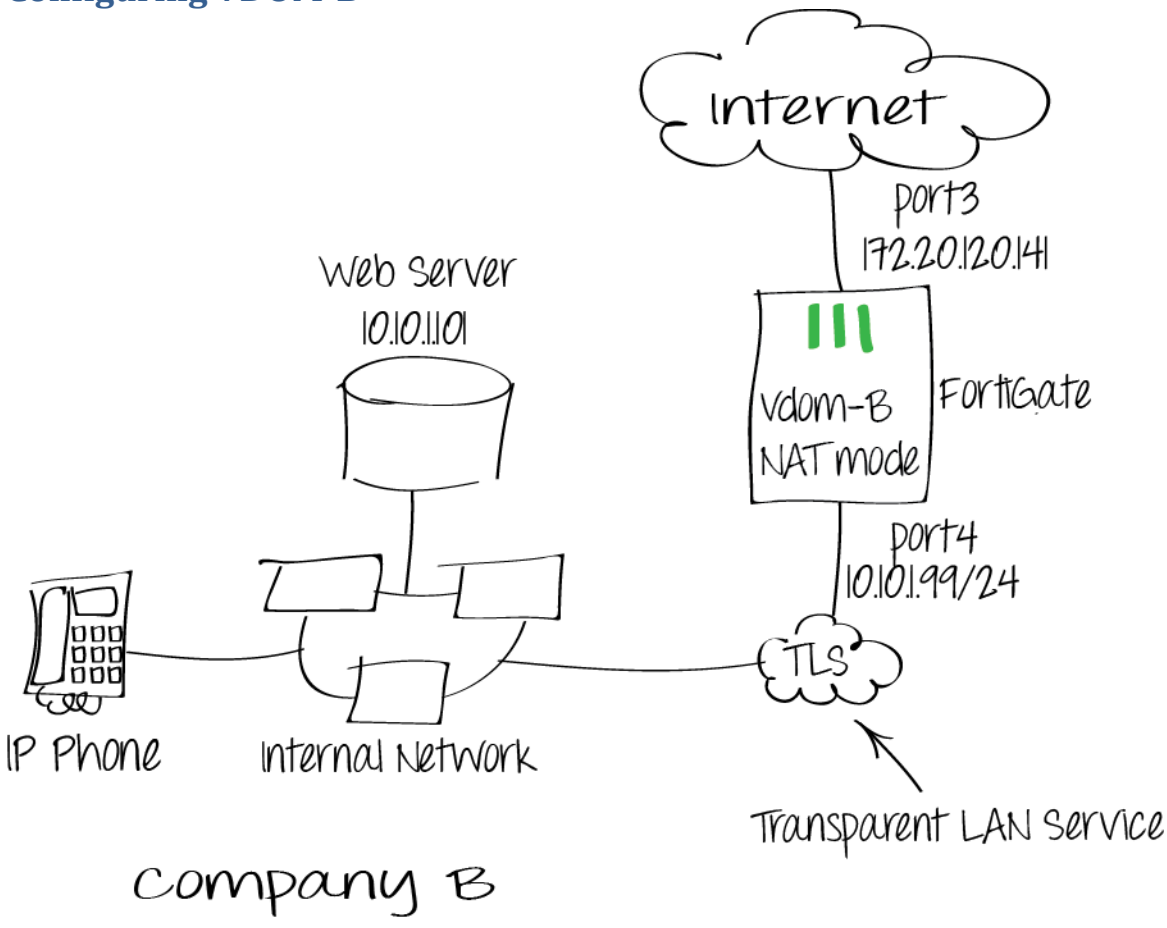


#	Date/Time	Src Interface	Dst Interface	Src	Dst	Policy ID	Service	Sent / Received
23	3 seconds ago	Engineering net	port1	192.168.10.2	65.55.239.146	1	HTTP	0 B / 0 B
24	3 seconds ago	Engineering net	port1	192.168.10.2	64.4.11.30	1	HTTP	0 B / 0 B
25	3 seconds ago	Engineering net	port1	192.168.10.2	64.4.11.30	1	HTTP	0 B / 0 B
26	7 seconds ago	Marketing net	port1	192.168.20.2	157.55.130.166	2	40021/udp	181 B / 49 B
27	7 seconds ago	Engineering net	port1	192.168.10.2	74.125.226.78	1	HTTPS	22.84 KB / 1.23 MB
28	10 seconds ago	Sales net	port1	192.168.30.2	74.217.240.83	3	HTTP	666 B / 2.60 KB
29	10 seconds ago	Sales net	port1	192.168.30.2	74.217.240.83	3	HTTP	727 B / 1.48 KB
30	10 seconds ago	Sales net	port1	192.168.30.2	54.243.35.93	3	HTTP	771 B / 453 B
31	12 seconds ago	Marketing net	port1	192.168.20.2	10.1.1.30	2	7836/udp	426 B / 0 B
32	12 seconds ago	Sales net	port1	192.168.30.2	12.129.199.104	3	HTTP	656 B / 491 B
33	13 seconds ago	Sales net	port1	192.168.30.2	54.243.35.93	3	HTTP	0 B / 0 B
34	16 seconds ago	Sales net	port1	192.168.30.2	72.246.43.67	3	HTTP	0 B / 0 B
35	16 seconds ago	Sales net	port1	192.168.30.2	157.166.224.246	3	HTTP	1.96 KB / 5.08 KB
36	17 seconds ago	Marketing net	port1	192.168.20.2	157.55.235.146	2	40046/udp	179 B / 71 B
37	17 seconds ago	Marketing net	port1	192.168.20.2	157.55.235.158	2	40045/udp	171 B / 85 B
38	17 seconds ago	Sales net	port1	192.168.30.2	157.166.255.219	3	HTTP	3.18 KB / 4.28 KB
39	17 seconds ago	Marketing net	port1	192.168.20.2	213.199.179.140	2	40041/udp	175 B / 84 B
40	17 seconds ago	Marketing net	port1	192.168.20.2	213.199.179.141	2	40021/udp	62 B / 490 B
41	17 seconds ago	Marketing net	port1	192.168.20.2	213.199.179.156	2	40001/udp	176 B / 49 B

Select an entry for more details

Dst	157.55.130.166	**Virtual Domain**	VDOM-A
Received	49	**Source Country**	Reserved
Src NAT IP	172.20.120.140	**Sent / Received**	181 B / 49 B
Duration	181	**Sent**	181
Src NAT Port	37023	**Application Details**	
Service	40021/udp	**Protocol**	17
Destination Country	United States	**Dst Port**	40021
roll	65534	**Status**	accept
Timestamp	Thu Dec 20 07:35:55 2012	**Tran Display**	snat
Sequence Number	369015	**Policy ID**	2
Src Interface	Marketing net	**Src**	192.168.20.2
Sent Packets	1	**Level**	notice
Src Port	37023	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	1	**Date/Time**	7 seconds ago (Thu Dec 20 07:35:55 2012)
Dst Interface	port1		

5. Configuring VDOM-B



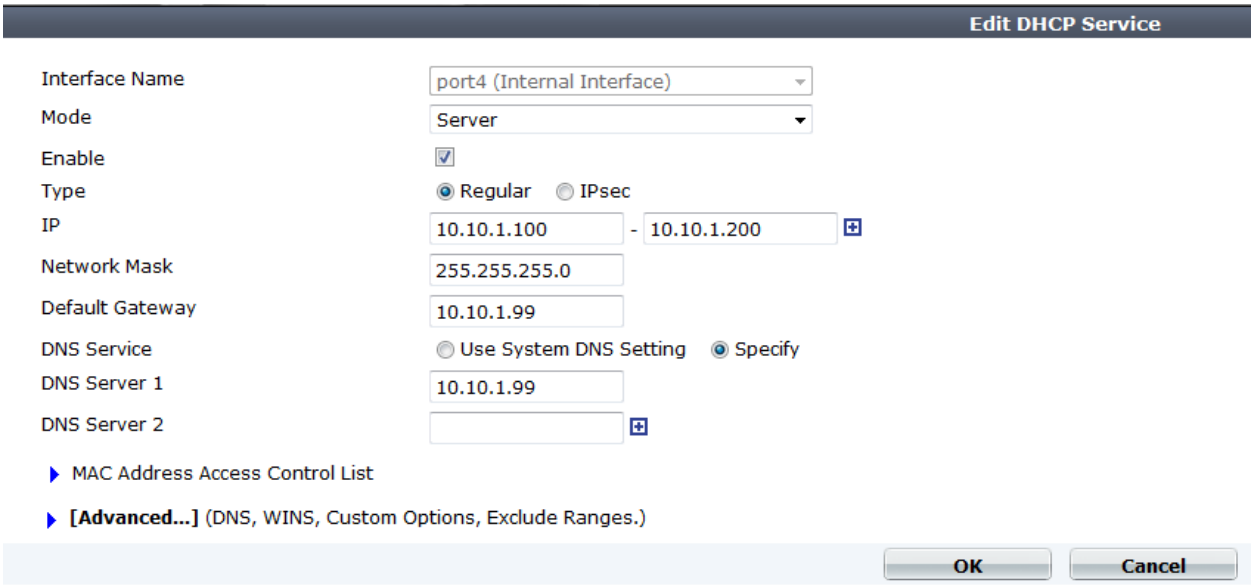
Log on to the FortiGate unit VDOM-B on port3 or port4 interface using b-admin account, this will let you manage only VDOM-B

Company B requires reserved IP according to device MAC address using DHCP, local DNS server, guaranteed bandwidth for sensitive traffic and faster web browsing. Consequently the following features will be covered:

- DHCP server to assign some IP addresses according to device MAC addresses
- Local DNS server listing for internal web sites and servers
- Traffic shaping to make sure high-priority services always have enough bandwidth
- Explicit web proxy and web caching users on some networks

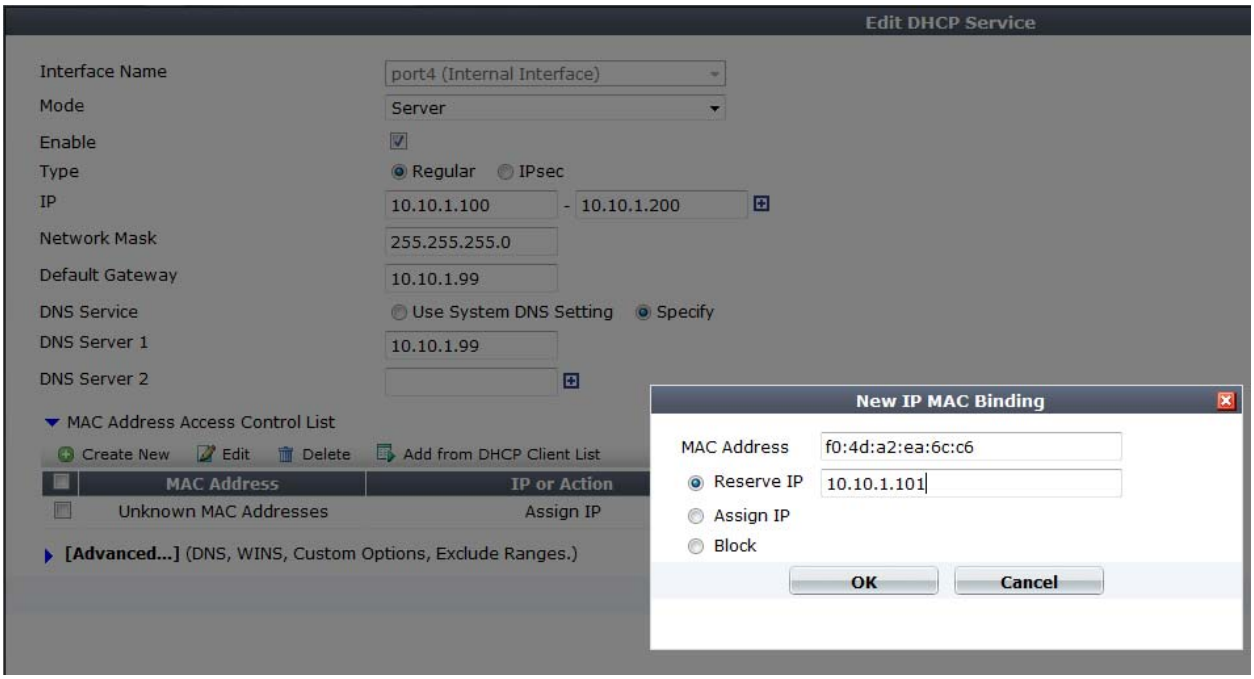
6. Configure DHCP to assign some IP addresses according to device MAC addresses

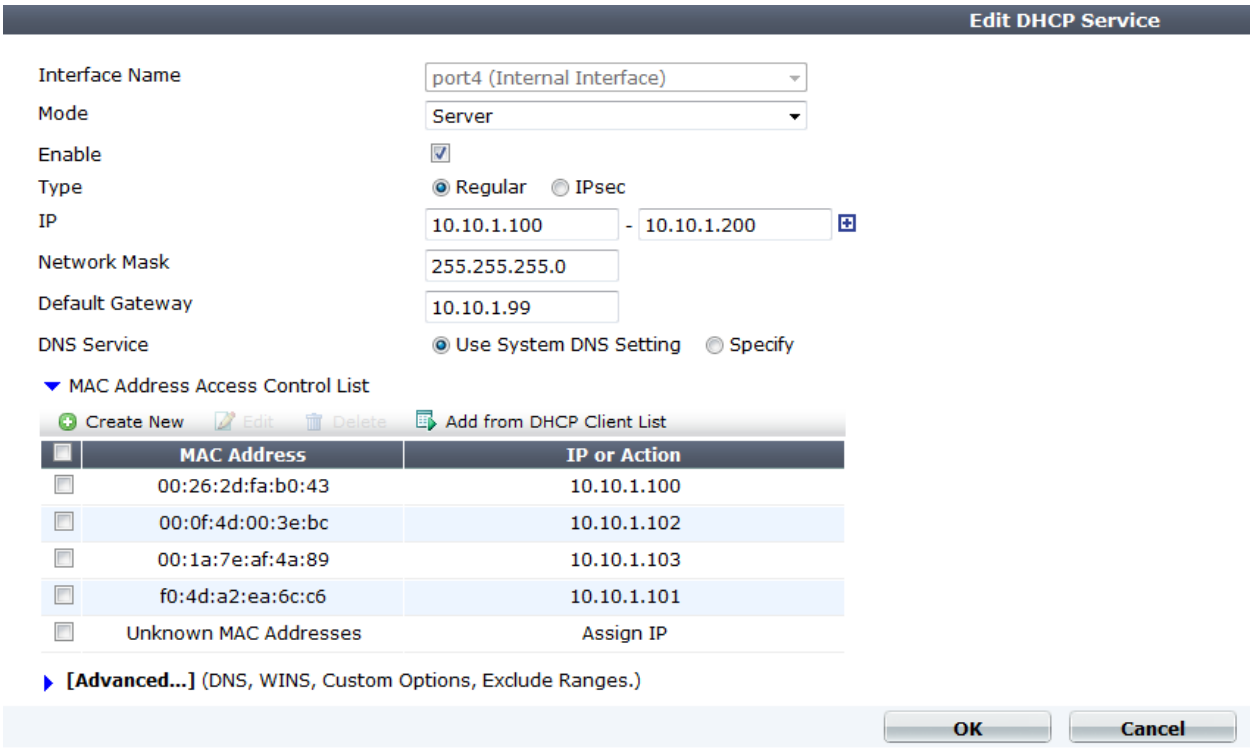
Go to System > Network > DHCP Server and add new for the internal interface (port4)



Make sure to specify the DNS Server to the internal IP of the FortiGate VDOM-B (10.10.1.99). This will be useful to resolve internal DNS requests

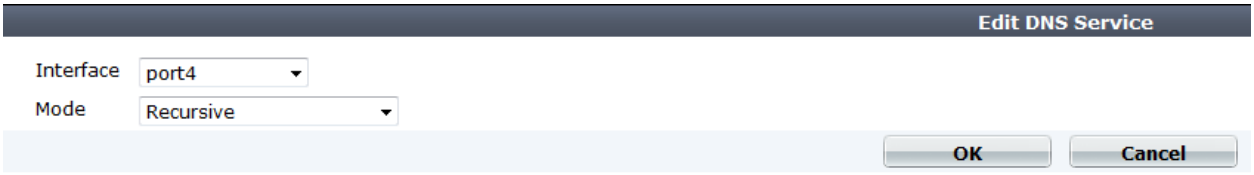
Extend “MAC Address Access Control List” and create a new then enter the MAC address of the device and its desired reserved IP address. You can also use “Add from DHCP Client List”


Edit DHCP Service
Interface Name
port4 (Internal Interface)
Mode
Server
Enable
Type
Regular
IPsec
IP
10.10.1.100
10.10.1.200
Network Mask
255.255.255.0
Default Gateway
10.10.1.99
DNS Service
Use System DNS Setting
Specify
DNS Server 1
10.10.1.99
DNS Server 2
MAC Address Access Control List
Create New
Edit
Delete
Add from DHCP Client List
MAC Address
IP or Action
Unknown MAC Addresses
Assign IP
[Advanced...] (DNS, WINS, Custom Options, Exclude Ranges.)
New IP MAC Binding
MAC Address
f0:4d:a2:ea:6c:c6
Reserve IP
10.10.1.101
Assign IP
Block
OK
Cancel


Edit DHCP Service
Interface Name
port4 (Internal Interface)
Mode
Server
Enable
Type
Regular
IPsec
IP
10.10.1.100
10.10.1.200
Network Mask
255.255.255.0
Default Gateway
10.10.1.99
DNS Service
Use System DNS Setting
Specify
MAC Address Access Control List
Create New
Edit
Delete
Add from DHCP Client List
MAC Address
IP or Action
00:26:2d:fa:b0:43
10.10.1.100
00:0f:4d:00:3e:bc
10.10.1.102
00:1a:7e:af:4a:89
10.10.1.103
f0:4d:a2:ea:6c:c6
10.10.1.101
Unknown MAC Addresses
Assign IP
[Advanced...] (DNS, WINS, Custom Options, Exclude Ranges.)
OK
Cancel

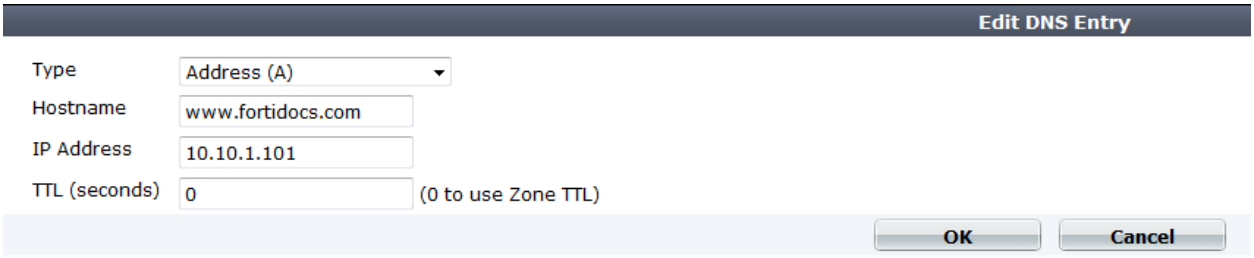
7. Creating a local DNS server listing for internal web sites and servers

Go to System > Network > DNS Server and create new under “DNS Service on Interface”. Make sure to set Mode to Recursive

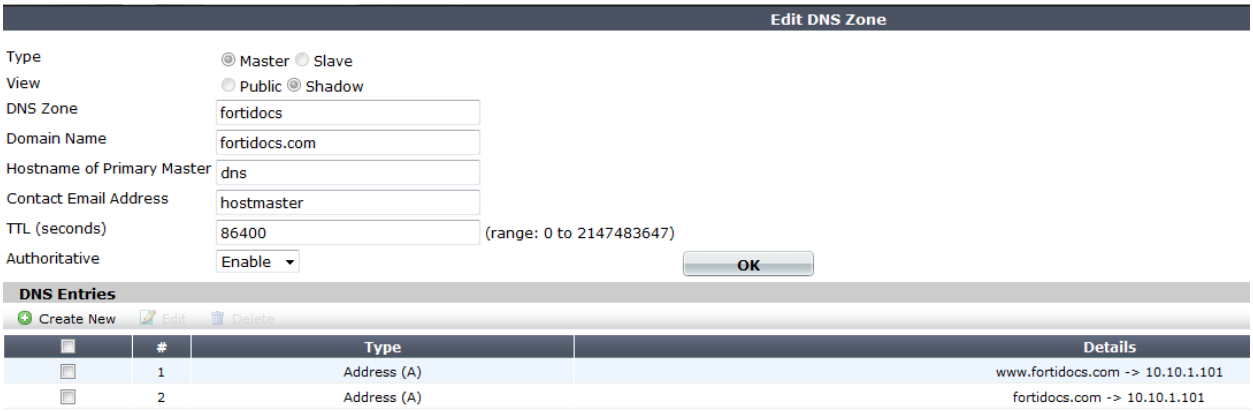


Then create new under “DNS Database” and add DNS Zone and Domain Name

Then create new under “DNS Entries” and add hostnames



The DNS zone will be looking like following:



From any host on the internal network, set your network connections to use the internal interface of FortiGate VDOM-B IP address (10.10.1.99) as a primary DNS server, then you will be able to surf to the web server using its IP address (10.10.1.101) and its domain name (fortidocs.com or www.fortidocs.com)

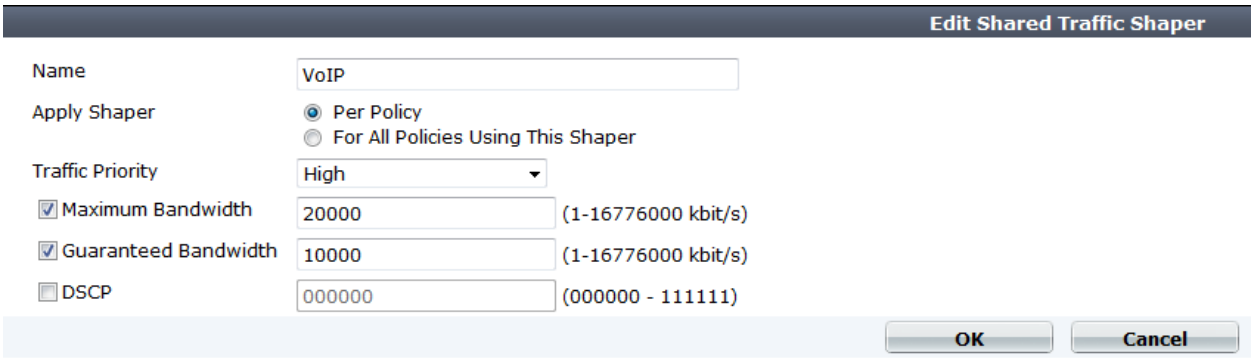
8. Configuring guaranteed bandwidth for sensitive traffic using traffic shaping

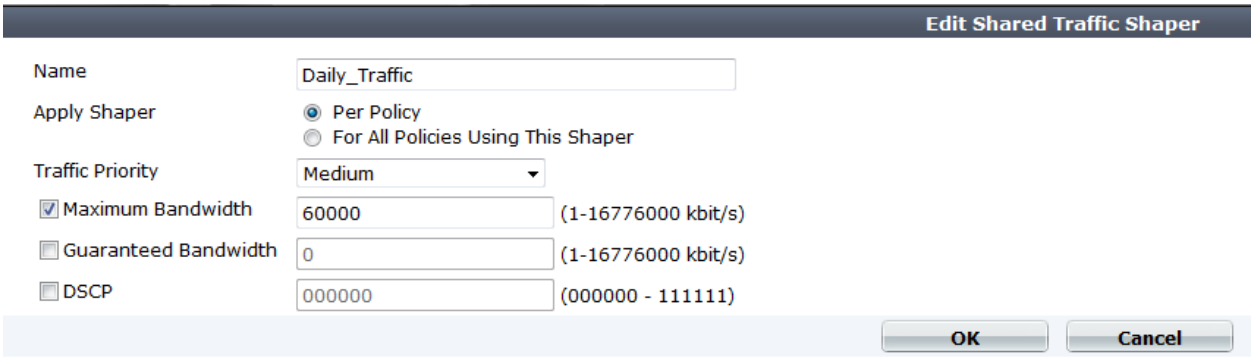
Sensitive traffic, such as VoIP, flowing through the Fortigate VDOM-B needs to have enough guaranteed bandwidth to assure the voice quality.

This scenario involves traffic shaping for VoIP/SIP traffic. To see how to configure SIP on the FortiGate unit, refer to “Allowing inbound and outbound VoIP/SIP traffic through the FortiGate” recipe.

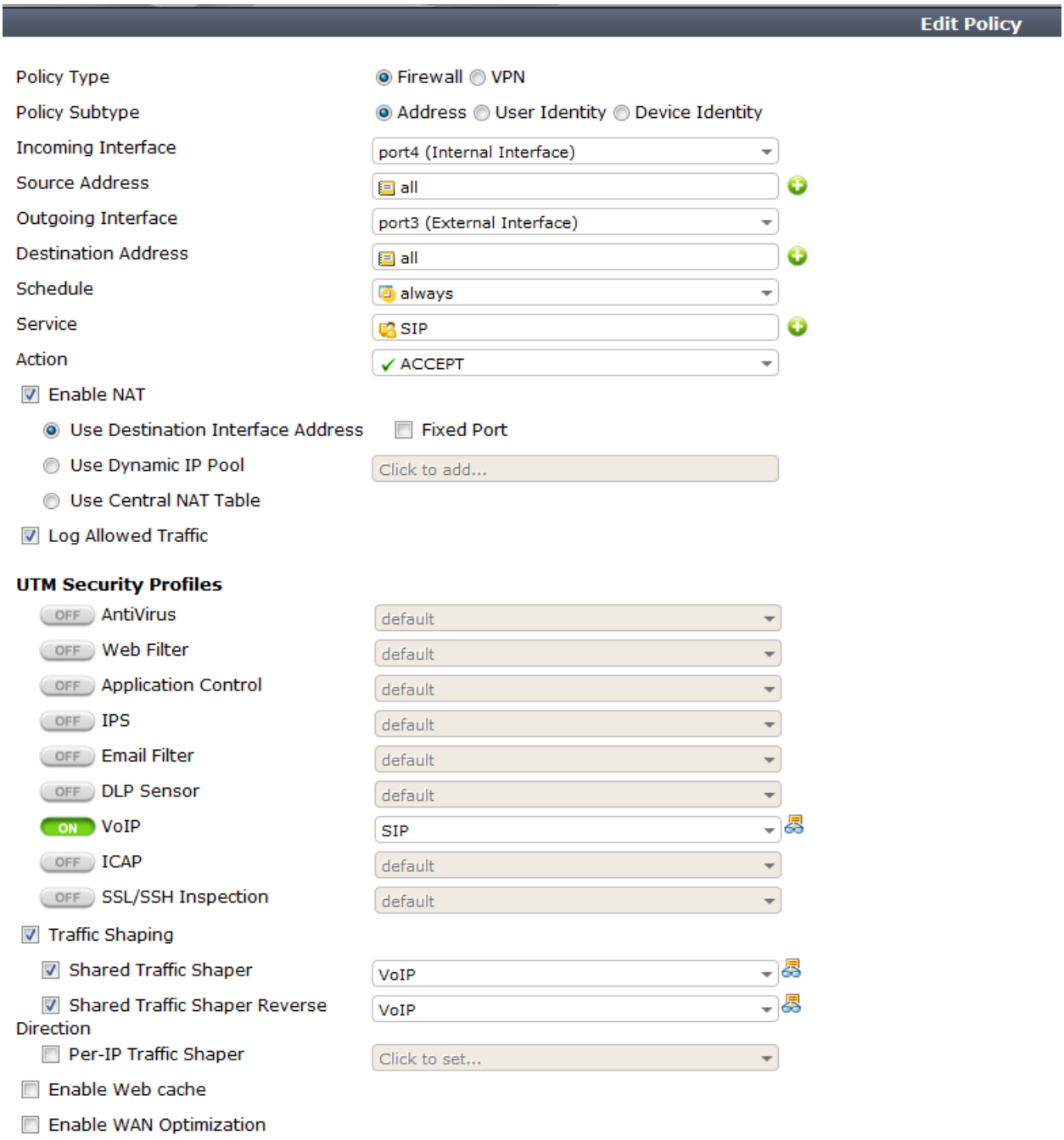
Using traffic shaping, you can configure shared shapers that ensure a consistent amount of reserved bandwidth for VoIP/SIP communications and still maintain bandwidth for other Internet traffic such as email and web browsing. Depends the total available bandwidth you have you can dedicate a guaranteed and a maximum bandwidth for each firewall policy (you can verify your total bandwidth using http://speedtest.net/). For this solution, total available bandwidth is 70000 Kbits/s, 10000 kbits/s is guaranteed to be available for VoIP and VoIP traffic is given higher priority than other traffic. Other traffic is limited to a maximum bandwidth of 600000 kbits/s.
In this configuration the internal IP phones and internal network are connected to the FortiGate VDOM-B internal interface (port4).

Go to Firewall Objects > Traffic Shaper > Shared and VoIP and Daily_Traffic Shapers

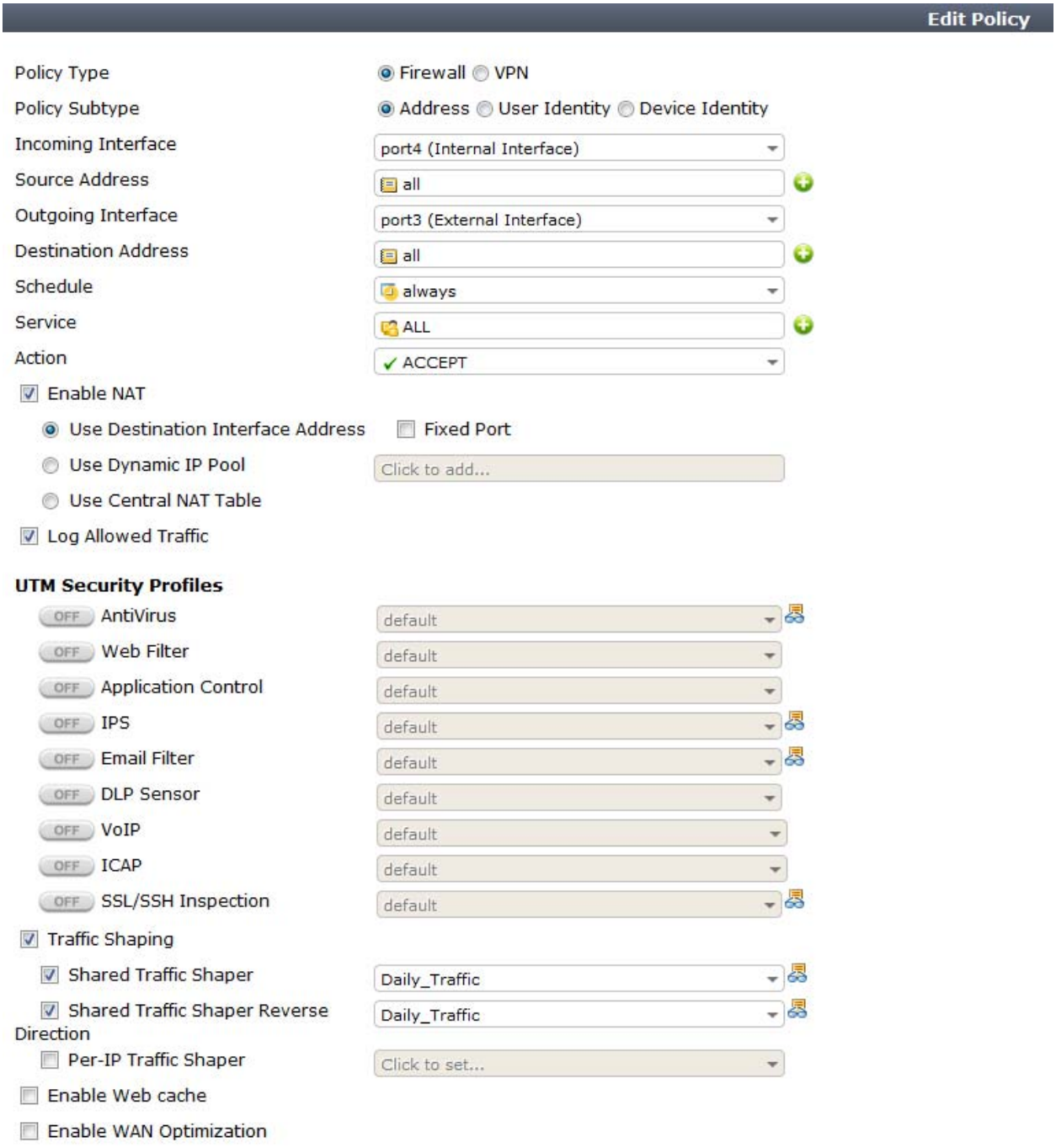




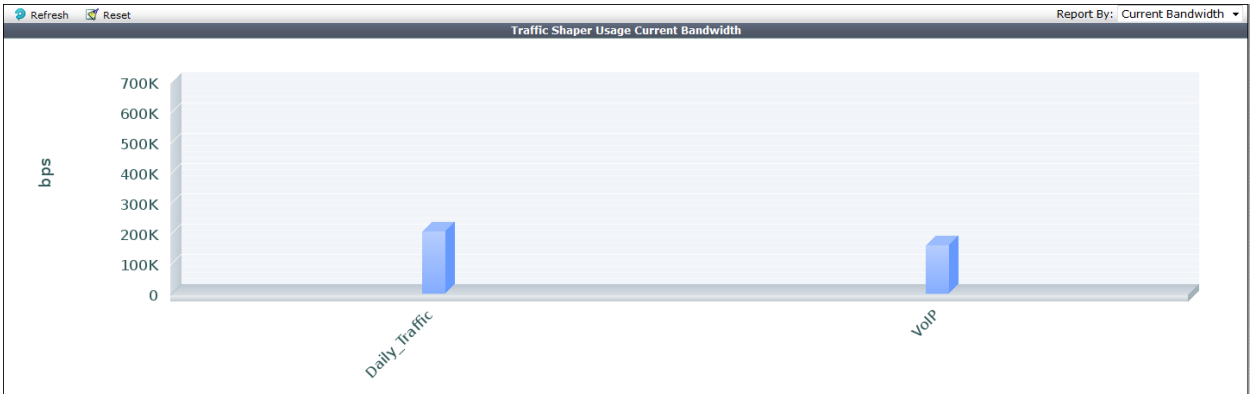
Go to Policy > Policy > Policy and apply the VoIP traffic shaper to the firewall policy controlling VoIP/SIP traffic



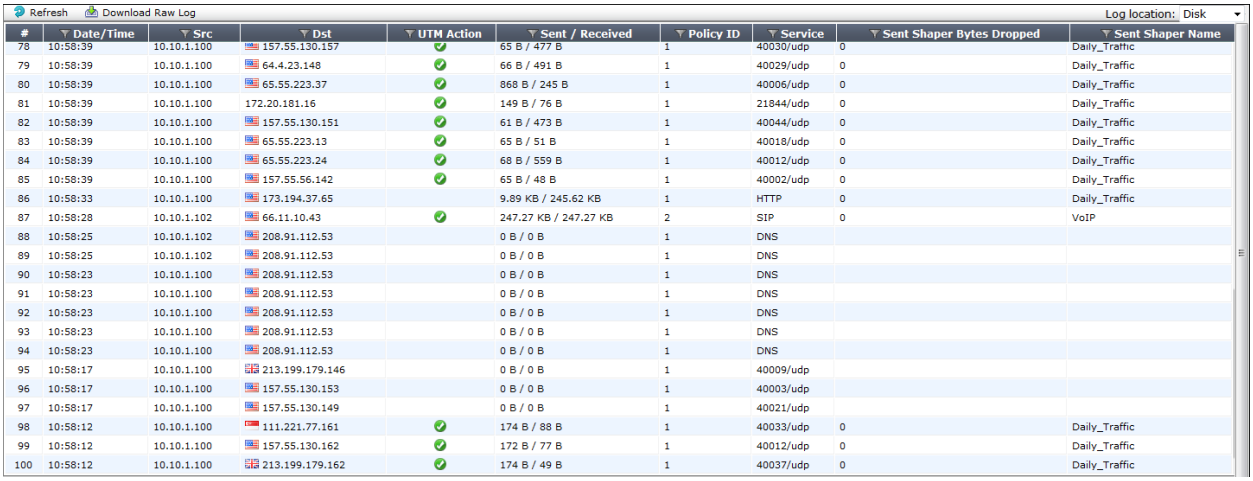
Then apply the Daily_Traffic shaper to the firewall policy controlling other traffic



Go to Firewall Objects > Monitor > Traffic Shaper Monitor



Go to Log & Report > Traffic Log > Forward Traffic to see that VoIP and Daily_Traffic shapers were applied successfully



#	Date/Time	Src	Dst	UTM Action	Sent / Received	Policy ID	Service	Sent Shaper Bytes Dropped	Sent Shaper Name
78	10:58:39	10.10.1.100	157.55.130.157	✓	65 B / 477 B	1	40030/udp	0	Daily_Traffic
79	10:58:39	10.10.1.100	64.4.23.148	✓	66 B / 491 B	1	40029/udp	0	Daily_Traffic
80	10:58:39	10.10.1.100	65.55.223.37	✓	868 B / 245 B	1	40006/udp	0	Daily_Traffic
81	10:58:39	10.10.1.100	172.20.181.16	✓	149 B / 76 B	1	21844/udp	0	Daily_Traffic
82	10:58:39	10.10.1.100	157.55.130.151	✓	61 B / 473 B	1	40044/udp	0	Daily_Traffic
83	10:58:39	10.10.1.100	65.55.223.13	✓	65 B / 51 B	1	40018/udp	0	Daily_Traffic
84	10:58:39	10.10.1.100	65.55.223.24	✓	68 B / 559 B	1	40012/udp	0	Daily_Traffic
85	10:58:39	10.10.1.100	157.55.56.142	✓	65 B / 48 B	1	40002/udp	0	Daily_Traffic
86	10:58:33	10.10.1.100	173.194.37.65		9.89 KB / 245.62 KB	1	HTTP	0	Daily_Traffic
87	10:58:28	10.10.1.102	66.11.10.43	✓	247.27 KB / 247.27 KB	2	SIP	0	VoIP
88	10:58:25	10.10.1.102	208.91.112.53		0 B / 0 B	1	DNS		
89	10:58:25	10.10.1.102	208.91.112.53		0 B / 0 B	1	DNS		
90	10:58:23	10.10.1.100	208.91.112.53		0 B / 0 B	1	DNS		
91	10:58:23	10.10.1.100	208.91.112.53		0 B / 0 B	1	DNS		
92	10:58:23	10.10.1.100	208.91.112.53		0 B / 0 B	1	DNS		
93	10:58:23	10.10.1.100	208.91.112.53		0 B / 0 B	1	DNS		
94	10:58:23	10.10.1.100	208.91.112.53		0 B / 0 B	1	DNS		
95	10:58:17	10.10.1.100	213.199.179.146		0 B / 0 B	1	40009/udp		
96	10:58:17	10.10.1.100	157.55.130.153		0 B / 0 B	1	40003/udp		
97	10:58:17	10.10.1.100	157.55.130.149		0 B / 0 B	1	40021/udp		
98	10:58:12	10.10.1.100	111.221.77.161	✓	174 B / 88 B	1	40033/udp	0	Daily_Traffic
99	10:58:12	10.10.1.100	157.55.130.162	✓	172 B / 77 B	1	40012/udp	0	Daily_Traffic
100	10:58:12	10.10.1.100	213.199.179.162	✓	174 B / 49 B	1	40037/udp	0	Daily_Traffic

Select an entry for each shaper to see details

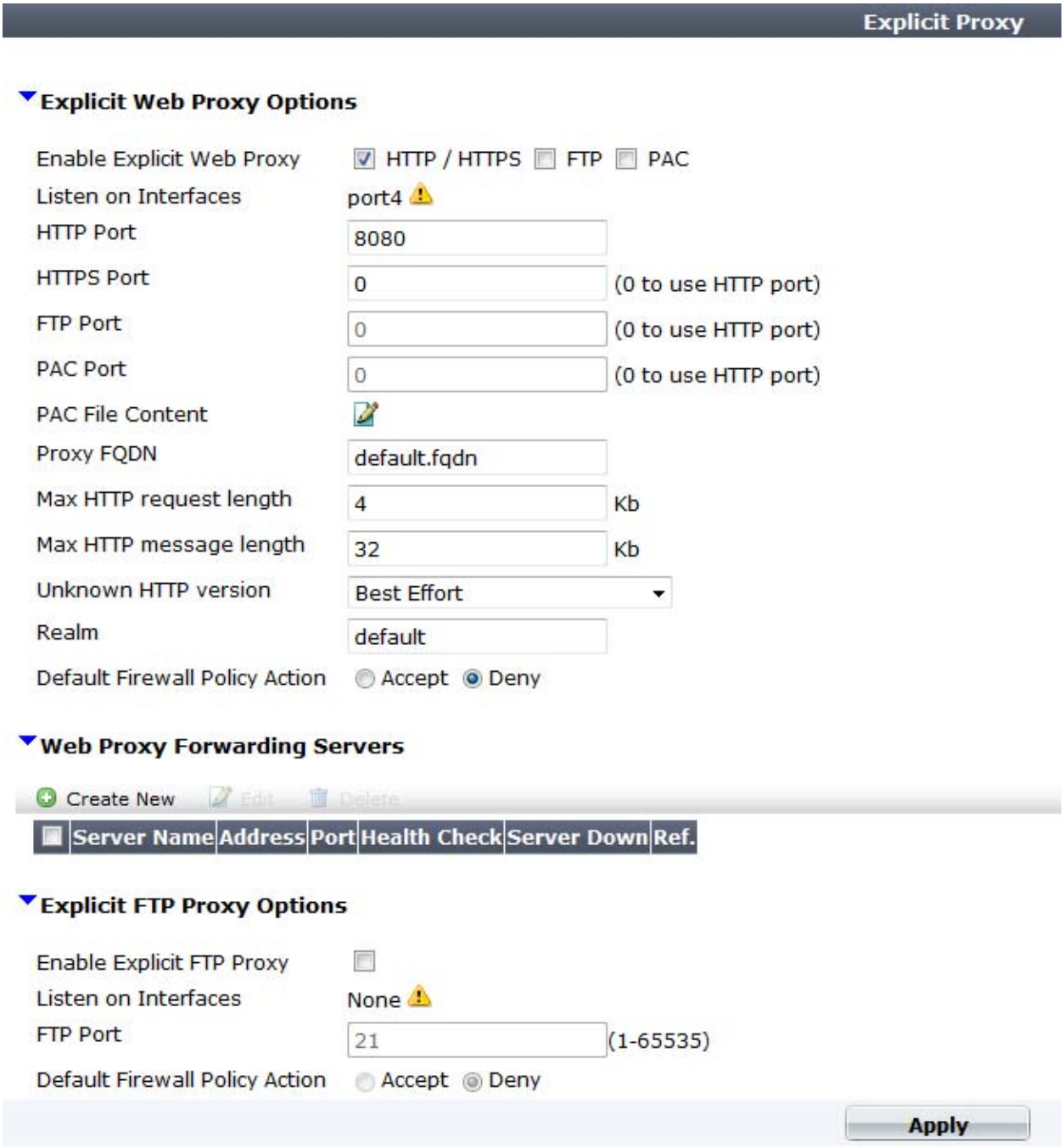
Dst	66.11.10.43	**Virtual Domain**	VDOM-B
Received	253200	**Source Country**	Reserved
Application Name	unknown-12	**Src NAT IP**	172.20.120.141
Sent / Received	247.27 KB / 247.27 KB	**Duration**	25
Sent	253200	**Sent Shaper Bytes Dropped**	0
Src NAT Port	6118	**Application Details**	
Service	SIP	**Protocol**	17
Sent Shaper Name	VoIP	**Destination Country**	United States
Dst Port	18176	**roll**	65535
Status	✓	**Timestamp**	Thu Jan 31 10:58:28 2013
Tran Display	snat	**Application ID**	12
Sequence Number	923	**Received Shaper Bytes Dropped**	0
Policy ID	2	**Src Interface**	port4
Src	10.10.1.102	**Sent Packets**	1266
Level	notice	**Received Shaper Name**	VoIP
Src Port	6100	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	1266	**Date/Time**	10:58:28 (Thu Jan 31 10:58:28 2013)
Dst Interface	port3		

Dst	173.194.37.65	**Virtual Domain**	VDOM-B
Received	251510	**Source Country**	Reserved
Sent Shaper Name	Daily_Traffic	**Src NAT IP**	172.20.120.141
Sent / Received	9.89 KB / 245.62 KB	**Duration**	77
Sent	10128	**Sent Shaper Bytes Dropped**	0
Src NAT Port	51054	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	65535	**Status**	close
Timestamp	Thu Jan 31 10:58:33 2013	**Tran Display**	snat
Sequence Number	9210	**Received Shaper Bytes Dropped**	0
Policy ID	1	**Src Interface**	port4
Src	10.10.1.100	**Sent Packets**	147
Level	notice	**Received Shaper Name**	Daily_Traffic
Src Port	51054	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	180	**Date/Time**	10:58:33 (Thu Jan 31 10:58:33 2013)
Dst Interface	port3		

9. Adding the explicit web proxy and web caching on the internal network

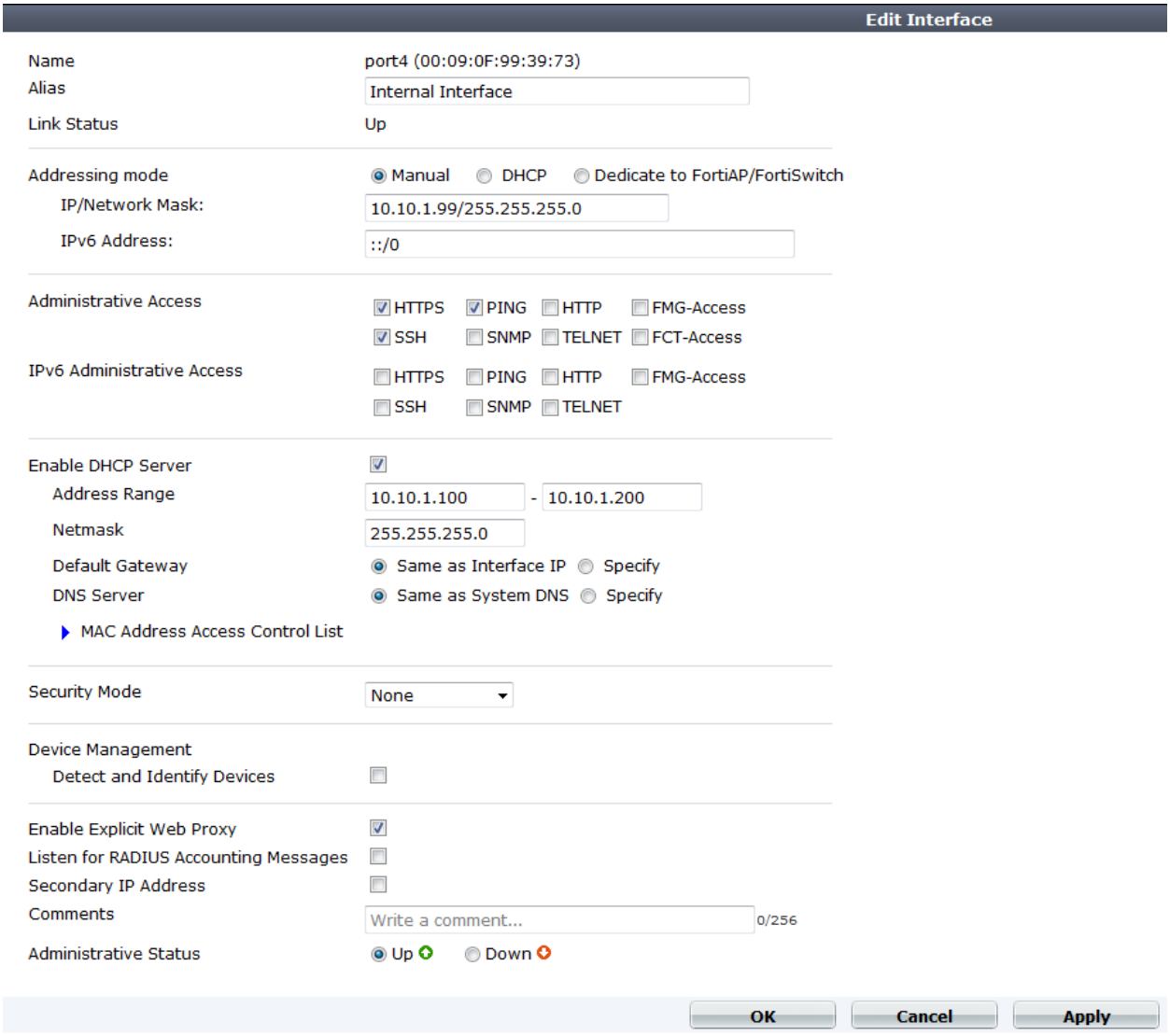
For faster web browsing, internal users will connect to an explicit web proxy using port 8080 instead of surfing directly to the Internet using port 80

Go to System > Network > Explicit Proxy and enable http/https explicit web proxy

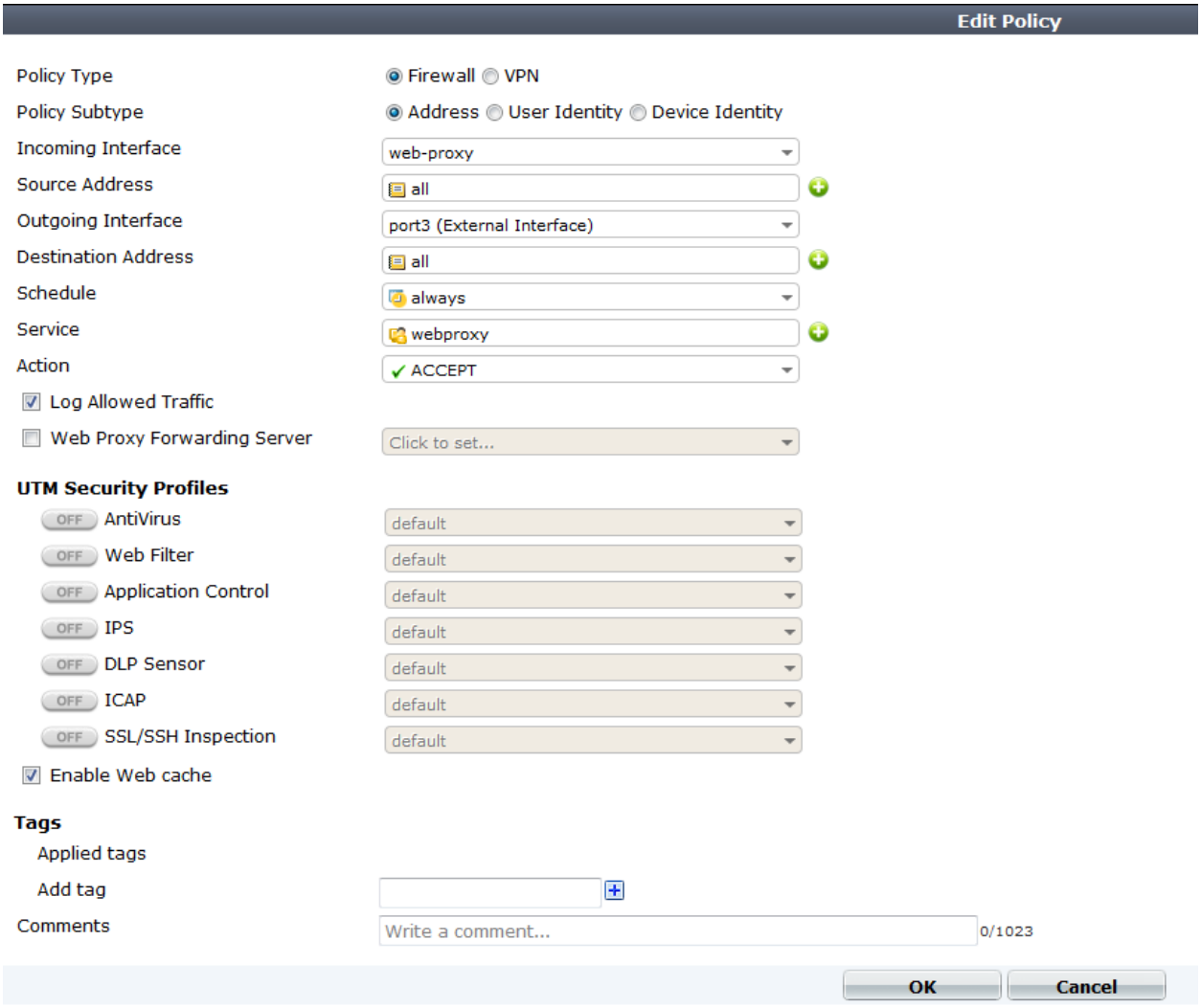


Make sure to set the Default Firewall Policy Action here to Deny, because we will create a policy for webproxy traffic with web cache enabled on it.

Go to System > Network > Interface and enable web proxy on port4


Edit Interface
Name
port4 (00:09:0F:99:39:73)
Alias
Internal Interface
Link Status
Up
Addressing mode
Manual
DHCP
Dedicate to FortiAP/FortiSwitch
IP/Network Mask:
10.10.1.99/255.255.255.0
IPv6 Address:
::/0
Administrative Access
HTTPS
PING
HTTP
FMG-Access
SSH
SNMP
TELNET
FCT-Access
IPv6 Administrative Access
HTTPS
PING
HTTP
FMG-Access
SSH
SNMP
TELNET
Enable DHCP Server
Address Range
10.10.1.100
10.10.1.200
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Specify
MAC Address Access Control List
Security Mode
None
Device Management
Detect and Identify Devices
Enable Explicit Web Proxy
Listen for RADIUS Accounting Messages
Secondary IP Address
Comments
Write a comment...
0/256
Administrative Status
Up
Down
OK
Cancel
Apply

Go to Policy > Policy > Policy to create new one for webproxy traffic and enable web cache



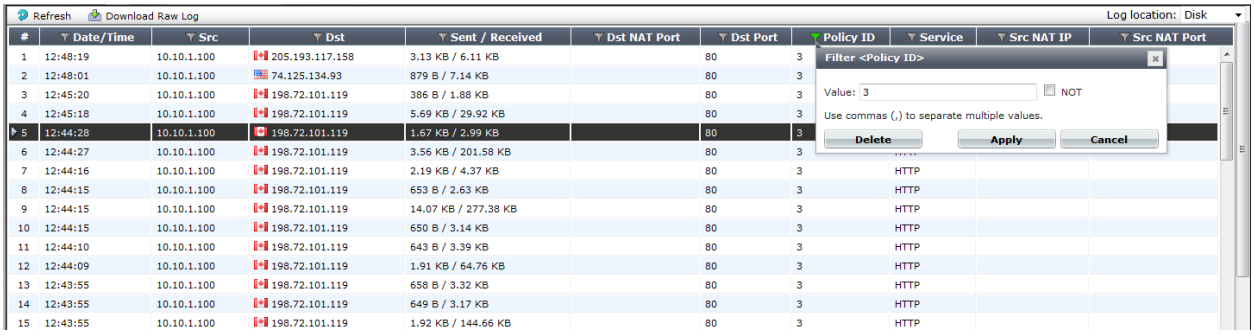
Configure web browsers on the private network to connect to the network using a proxy server. The IP address of the HTTP proxy server is 10.10.1.99 (the IP address of the FortiGate internal interface) and the port is 8080 (the default explicit web proxy port).

Web browsers configured to use the proxy server are able to connect to the Internet.

Go to policy > Policy > Policy to see the ID of the policy allowing webproxy traffic (here it's ID 3)

Web proxy traffic is not counted by firewall policy!

Go to Log & Report > Traffic Log > Forward Traffic and filter by policy ID 3



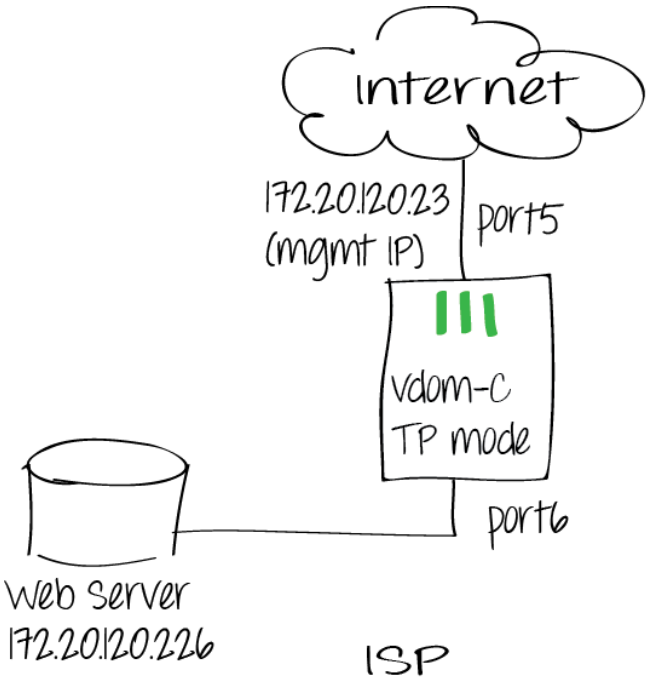
#	Date/Time	Src	Dst	Sent / Received	Dst NAT Port	Dst Port	Policy ID	Service	Src NAT IP	Src NAT Port
1	12:48:19	10.10.1.100	205.193.117.158	3.13 KB / 6.11 KB		80	3			
2	12:48:01	10.10.1.100	74.125.134.93	879 B / 7.14 KB		80	3			
3	12:45:20	10.10.1.100	198.72.101.119	386 B / 1.88 KB		80	3			
4	12:45:18	10.10.1.100	198.72.101.119	5.69 KB / 29.92 KB		80	3			
5	12:44:28	10.10.1.100	198.72.101.119	1.67 KB / 2.99 KB		80	3			
6	12:44:27	10.10.1.100	198.72.101.119	3.56 KB / 201.58 KB		80	3			
7	12:44:16	10.10.1.100	198.72.101.119	2.19 KB / 4.37 KB		80	3	HTTP		
8	12:44:15	10.10.1.100	198.72.101.119	653 B / 2.63 KB		80	3	HTTP		
9	12:44:15	10.10.1.100	198.72.101.119	14.07 KB / 277.38 KB		80	3	HTTP		
10	12:44:15	10.10.1.100	198.72.101.119	650 B / 3.14 KB		80	3	HTTP		
11	12:44:10	10.10.1.100	198.72.101.119	643 B / 3.39 KB		80	3	HTTP		
12	12:44:09	10.10.1.100	198.72.101.119	1.91 KB / 64.76 KB		80	3	HTTP		
13	12:43:55	10.10.1.100	198.72.101.119	658 B / 3.32 KB		80	3	HTTP		
14	12:43:55	10.10.1.100	198.72.101.119	649 B / 3.17 KB		80	3	HTTP		
15	12:43:55	10.10.1.100	198.72.101.119	1.92 KB / 144.66 KB		80	3	HTTP		

Select an entry for details

Dst	198.72.101.119	**Virtual Domain**	VDOM-B
Received	3057	**WAN In**	3057
Sent / Received	1.67 KB / 2.99 KB	**WAN Opt Application Category**	web-cache
Duration	34	**Sent**	1712
Application Details		**LAN Out**	4693
Source Country	Reserved	**Service**	HTTP
Destination Country	Canada	**Dst Interface**	port3
Dst Port	80	**roll**	65530
Timestamp	Tue Jan 22 12:44:28 2013	**LAN In**	1712
Src Interface	port4	**Src**	10.10.1.100
Level	notice	**Src Port**	53859
logid	9	**Sub Type**	forward
Threat		**WAN Out**	1238
Date/Time	12:44:28 (Tue Jan 22 12:44:28 2013)	**Policy ID**	3

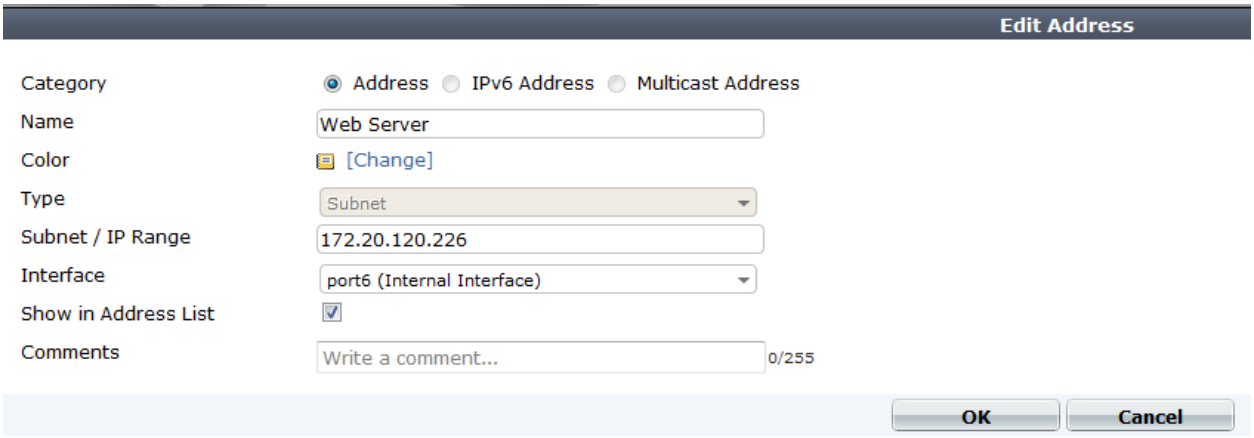
10. Configuring VDOM-C

This VDOM-C in transparent mode will be set to protect the ISP's servers set to public IPs using UTM Profiles

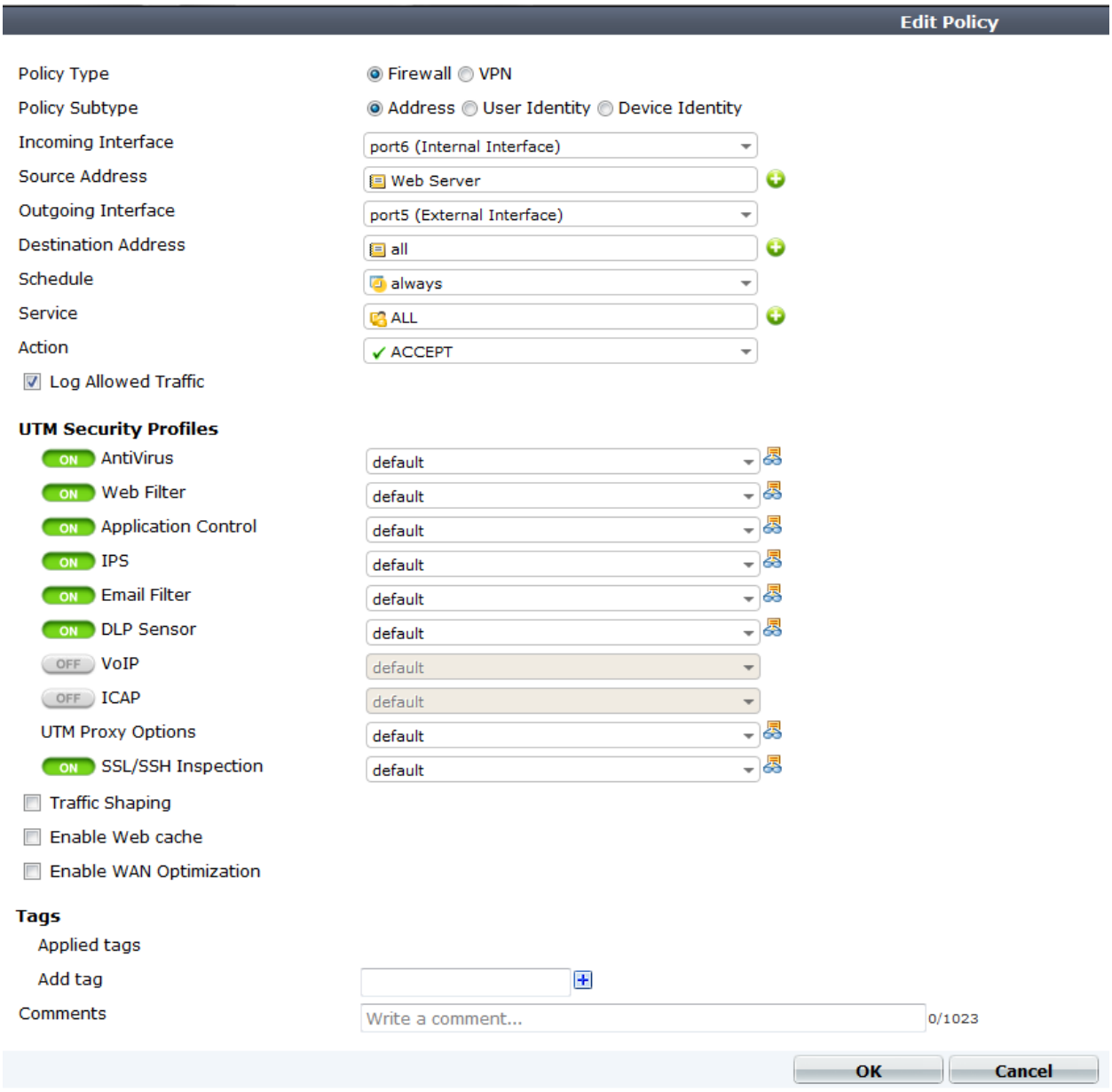


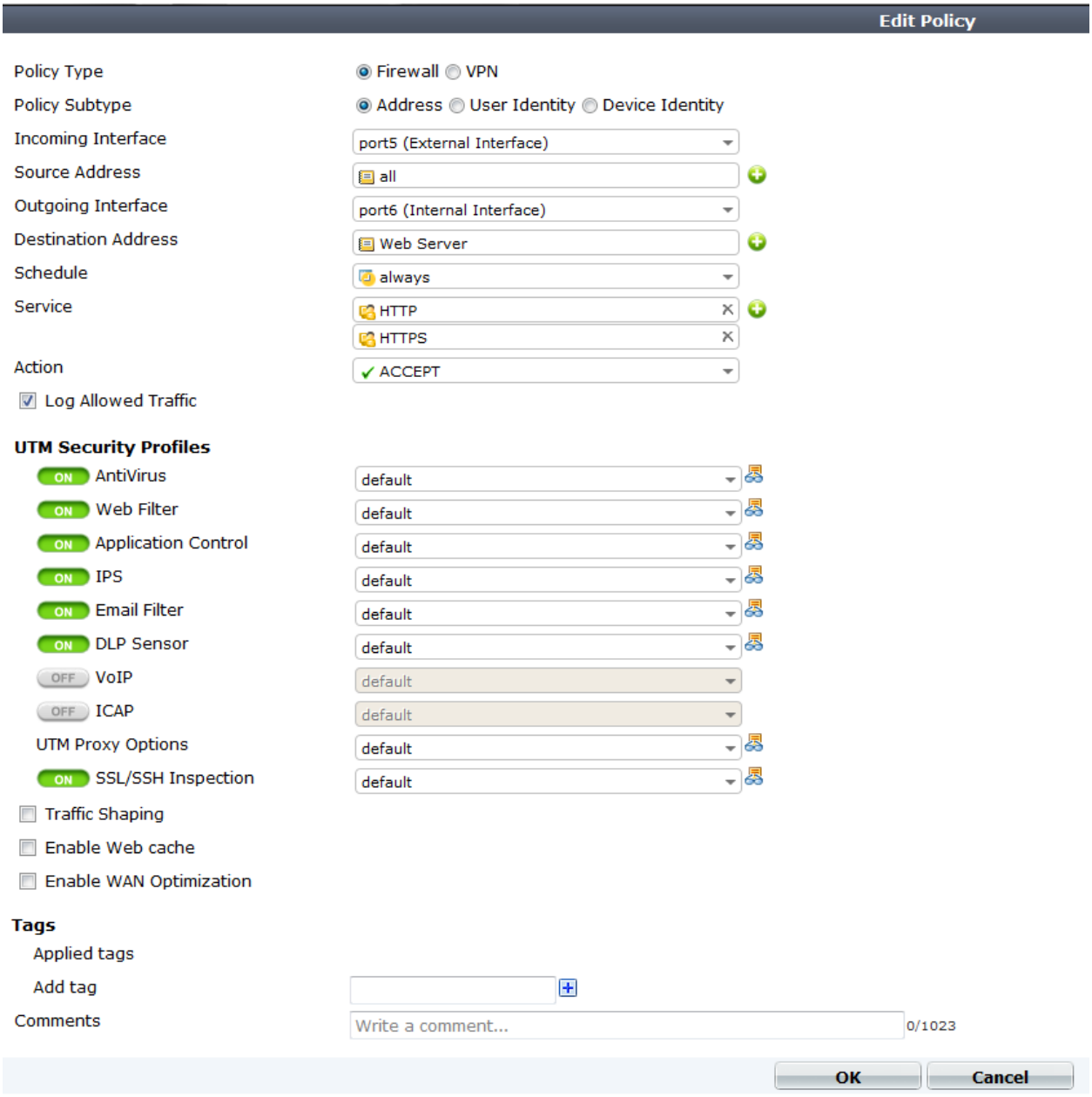
Log on to the FortiGate unit VDOM-C on port5 interface (management IP 172.20.120.23) using c-admin account, this will let you manage only VDOM-C

Go to Firewall Objects > Address > Address to set web server IP



Go to Policy > Policy > Policy to create one for outbound traffic and apply UTM security profiles then another one for inbound traffic with security UTM profiles as well


Edit Policy
Policy Type
Firewall
VPN
Policy Subtype
Address
User Identity
Device Identity
Incoming Interface
port6 (Internal Interface)
Source Address
Web Server
Outgoing Interface
port5 (External Interface)
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Log Allowed Traffic
UTM Security Profiles
AntiVirus
default
Web Filter
default
Application Control
default
IPS
default
Email Filter
default
DLP Sensor
default
VoIP
default
ICAP
default
UTM Proxy Options
default
SSL/SSH Inspection
default
Traffic Shaping
Enable Web cache
Enable WAN Optimization
Tags
Applied tags
Add tag
Comments
Write a comment...
0/1023
OK
Cancel



You can use the default profiles and customize them if you want to.

You can now connect to your web server securely from the internet using its public IP address (eventually using the same FQDN) although the web server is behind a FortiGate unit. Also the web server is able to connect to the internet for updates and others.

Go to Log & Report > Traffic Log > Forward Traffic to see in and out bound traffic

Refresh | Download Raw Log | Log location: Disk

#	Date/Time	Src	Dst	Sent / Received	Dst Interface	Policy ID	Service	Src Interface
12	13:27:41	172.20.120.226	96.7.202.70	0 B / 0 B	port5	1	HTTPS	port6
13	13:27:41	172.20.120.226	192.168.110.9	0 B / 0 B	port5	1	ALL_UDP	port6
14	13:18:06	172.20.120.21	172.20.120.226	5.58 KB / 189.28 KB	port6	2	ALL_TCP	port5
15	13:17:55	172.20.120.226	132.246.2.9	9.00 KB / 377.01 KB	port5	1	ALL_TCP	port6
16	13:17:52	172.20.120.226	74.125.226.8	2.03 KB / 1.17 KB	port5	1	ALL_TCP	port6
17	13:17:41	172.20.120.226	74.125.226.8	0 B / 0 B	port5	1	ALL_TCP	port6
18	13:17:41	172.20.120.226	192.168.110.9	0 B / 0 B	port5	1	ALL_UDP	port6
19	13:15:55	172.20.120.226	157.56.67.222	93.43 KB / 15.21 KB	port5	1	HTTPS	port6
20	13:15:55	172.20.120.226	65.55.13.90	891 B / 960 B	port5	1	ALL_TCP	port6
21	13:15:04	172.20.120.21	172.20.120.226	839 B / 1.36 KB	port6	2	HTTPS	port5
22	13:15:02	172.20.120.21	172.20.120.226	839 B / 1.40 KB	port6	2	HTTPS	port5
23	13:14:57	172.20.120.21	172.20.120.226	799 B / 1.40 KB	port6	2	HTTPS	port5
24	13:14:56	172.20.120.226	157.56.67.222	2.19 KB / 4.30 KB	port5	1	HTTPS	port6
25	13:14:54	172.20.120.226	132.246.2.6	1.44 KB / 5.20 KB	port5	1	ALL_TCP	port6
26	13:14:55	172.20.120.226	132.246.2.6	1.73 KB / 5.51 KB	port5	1	ALL_TCP	port6
27	13:14:49	172.20.120.226	132.246.2.9	497 B / 363 B	port5	1	ALL_TCP	port6
28	13:14:48	172.20.120.226	132.246.2.9	0 B / 0 B	port5	1	ALL_TCP	port6
29	13:14:48	172.20.120.226	192.168.110.9	0 B / 0 B	port5	1	ALL_UDP	port6

Select an entry for outbound and another entry for inbound traffic for details

Dst	157.56.67.222	**Virtual Domain**	VDOM-C
Received	4406	**Source Country**	Reserved
Sent / Received	2.19 KB / 4.30 KB	**Duration**	11
Sent	2246	**Application Details**	
Service	HTTPS	**Protocol**	6
Destination Country	United States	**Dst Port**	443
roll	0	**Status**	close
Timestamp	Tue Jan 22 13:14:56 2013	**Tran Display**	noop
Sequence Number	18245	**Policy ID**	1
Src Interface	port6	**Src**	172.20.120.226
Sent Packets	9	**Level**	notice
Src Port	49284	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	7	**Date/Time**	13:14:56 (Tue Jan 22 13:14:56 2013)
Dst Interface	port5		

Dst	74.125.226.8	**Virtual Domain**	VDOM-C
Received	1199	**Source Country**	Reserved
Sent / Received	2.03 KB / 1.17 KB	**Duration**	11
Sent	2080	**Application Details**	
Service	ALL_TCP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	0	**Status**	close
Timestamp	Tue Jan 22 13:17:52 2013	**Tran Display**	noop
Sequence Number	18524	**Policy ID**	1
Src Interface	port6	**Src**	172.20.120.226
Sent Packets	5	**Level**	notice
Src Port	49286	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	4	**Date/Time**	13:17:52 (Tue Jan 22 13:17:52 2013)
Dst Interface	port5		

Go to UTM Security Profiles > Monitor to see all UTM status

Here is an example of Application monitor from that web server with IP address 172.20.120.226


Refresh
Reset
Top Applications Usage Monitor
Top Applications by Bandwidth
DNS
ICMP
DHCP
Bits per Second
Top Applications by Session Count
DNS
6
ICMP
1
DHCP
1
0 1 2 3 4 5 6 7 8 9 10
Top IP/User for DNS
172.20.120.226
7.9K
0 2K 4K 6K 8K 10K 12K 14K 16K 18K 20K
Bytes